République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Centre Universitaire Cheick Larbi Tébessi
TEBESSA

Département d'Informatique

Ecole Doctorale en Sciences et Technologies de l'Information et de la Communication (STIC)

MEMOIRE

Présenté en vue de l'obtention du diplôme de magister en informatique

Option : Informatique Répartie et Mobile (IRM)

PROBLEME DE SECURITE DANS LES RESEAUX MOBILES AD HOC

Par

Chahra LALAOUA

Proposé par

Professeur Mohammed BENMOHAMMED

Devant le jury d'examen:

Pr. BILAMI Azedine, Professeur à l'Université de Batna, Président.

Pr. BENMOHAMMED Mohammed, Professeur à l'Université de Constantine, Rapporteur.

Pr. CHAOUI Allaoua professeur à l'Université de Constantine, Examinateur.

Dr. LAOUAR Redha Maitre de conférences à l'Université de Tébessa, Examinateur.

Promotion 2012-2013

À tous Ceux que J'aime…

Remerciement

*En premier lieu, je remercie **le Bon Dieu** de m'avoir donné la force, la santé et le courage pour accomplir ce travail et qui m'a procuré ce succès.*

« On parvient rarement à ses fins par ses propres moyens ;
il faut toujours compter sur quelqu'un d'autre »
Marie-Claude Bussières-Tremblay.

Je tiens à exprimer tous mes sincères remerciements à mon promoteur le professeur : BENMOHAMMED Mohammed, pour avoir dirigé ce mémoire. Ses encouragements dans mes moments de doute et la confiance qu'il m'a accordée m'ont permis de mener à bien ce travail. Je tiens encore à lui exprimer mon grand respect, ma profonde gratitude pour son aide et tous ses précieux conseils.

Je remercie tout particulièrement les membres de mon jury de mémoire, qui ont accepté de juger ce travail et de participer au jury. J'adresse mes très sincères remerciements au Pr : BILAMI Azzedine, professeur à l'université de Batna, de me faire l'honneur de s'intéresser à ce travail et d'avoir présidé le jury. Merci au Pr. CHAOUI Allaoua professeur à l'Université de Constantine, Dr. LAOUAR Redha maitre de conférences à l'Université de Tebessa, qui m'ont fait l'honneur d'être les rapporteurs de ce mémoire.

« Soyons reconnaissants aux personnes qui nous donnent du bonheur ; elles sont les charmants Jardiniers par qui nos âmes sont fleuries. » Marcel Proust (1871-1922).

Je ne pourrais clôturer ces remerciements sans me retourner vers les êtres qui mes sont le plus chers, qui ont eu un rôle essentiel et continu pendant ma réussite, et qui sans eux aucune réussite n'aurait été possible. J'adresse de tout mon cœur mes remerciements à mes chers parents, mes sœurs et mes frères, je suis infiniment reconnaissante pour leurs amours et leurs soutiens morals aux moments les plus difficiles. Je veux leur dire que leurs beaux sourires seront toujours ma source d'espoir. Qu'ils trouvent dans ce travail le fruit de leur travail.

Merci du fond du cœur

RÉSUMÉ

Les progrès considérables des technologies de l'information et le penchant vers l'utilisation des machines sans fil qui se sont imposées ces dernières années ont fait émerger un nouveau type de réseaux : les réseaux sans-fil ad hoc, ou MANET (Mobile Ad hoc NETwork). Les réseaux ad hoc sont des systèmes autonomes composés par un ensemble d'entités mobiles libres de se déplacer sans contraintes, elles utilisent le médium radio pour communiquer. Ces entités fonctionnent sans l'utilisation d'aucune infrastructure existante. Avec cette contrainte, les nœuds doivent coopérer afin de fournir les fonctionnalités nécessaires du réseau. Un des principaux protocoles de routage utilisés dans les réseaux ad hoc est AODV (Ad hoc on demand Distance Vector). Cependant, La conception d'AODV a peu d'attention aux considérations de sécurité. La sécurité reste un défi majeur pour ces réseaux en raison de leurs caractéristiques de milieu ouvert, changement dynamique de topologie, l'absence des points de contrôle centralisés, et le manque de lignes de défense claires. Dans ce mémoire, un mécanisme de sécurité de routage basé sur l'écoute commune de voisinage est proposé. Dans ce mécanisme, la valeur de confiance est définie pour évaluer la réputation d'un nœud et juger si un nœud est un nœud malveillant ou non. Cette proposition peut renforcer la sécurité du protocole AODV (Ad hoc On-demand Distance Vector). Le mécanisme peut réagir rapidement pour protéger le réseau contre certain type d'attaques lorsque certains nœuds malveillants se produisent dans le réseau ad hoc. Une fois l'itinéraire est détruit par un nœud malveillant, le mécanisme de l'écoute commune de voisinage va chercher un autre itinéraire vers la destination pendant la phase de découverte de route. Les performances de ce mécanisme dans AODV sont justifiées par simulation.

MOTS-CLÉS : réseau MANET, AODV, sécurité, attaque, simulation.

ABSTRACT

Significant advancements in information technology and the use of wireless equipment have emerged in recent years have given rise to a new type of networks: Wireless ad hoc or MANET (Mobile Ad hoc NETwork). An ad hoc network is a collection of mobile nodes free to move that dynamically form a temporary network. They use the radio medium to communicate and operate without the use of existing infrastructure. In the absence of a fixed infrastructure, nodes have to cooperate in order to provide the necessary network functionality. One of the principal routing protocols used in Ad hoc networks is AODV (Ad hoc on demand Distance Vector) protocol. However, the design of AODV has little attention to security considerations. Security remains a major challenge for these networks due to their features of open medium, dynamically changing topologies, absence of centralized monitoring points, and lack of clear lines of defense. In this memory, a security routing mechanism based on common neighbor listening is proposed. This proposition can reinforce the security of AODV (Ad hoc On-demand Distance Vector). In this mechanism, the trust value is defined to evaluate a node's reputation and judge whether a node is a malicious node or not. The mechanism can react quickly for protect the network from kinds of attacks when some malicious nodes occur in the Ad hoc network. Once the route is destroyed by malicious node, common neighbor will search another route to the destination during a route discovery phase. The performance of this mechanism in AODV is justified by simulation.

KEYWORDS: MANET network, AODV, security, attack, simulation.

TABLE DES MATIERES

TABL DE FIGURES

LISTE DES TABLEAUX

INTRODUCTION GÉNÉRALE

Les réseaux informatiques constituent depuis quelques années un outil incontournable pour le transport de l'information où la diffusion de celle-ci ne cesse de s'imposer comme un des plus gros besoins de notre société. Avec l'avancement des technologies de l'information, nous entrons aujourd'hui dans une nouvelle ère technologique et de nouvelles attentes telles que la mobilité ont favorisé le développement des réseaux sans fil de façon remarquable.

L'essor de ces technologies sans fil, offre aujourd'hui de nouvelles perspectives dans le domaine des télécommunications. Notamment l'évolution récente des moyens de communication sans fil qui a permis la manipulation de l'information à travers des unités de calcul portables qui ont des caractéristiques particulières (une faible capacité de stockage, une source d'énergie autonome..) et accèdent au réseau à travers une interface de communication sans fil.

De plus, le penchant vers l'utilisation de ces machines sans fil ces dernières années a fait émerger un nouveau type de réseaux : les réseaux sans-fil Ad hoc, ou MANET (Mobile Ad hoc NETwork). L'aspect le plus novateur de ces réseaux est leur capacité à fournir une couverture réseau mobile de manière automatique et autonome, et ce même sans accès à une infrastructure préexistante. Dans tel réseau, tout le monde peut se communiquer et partager l'information dans n'importe quelle situation. De ce fait, les réseaux Ad hoc mobiles sont l'une des principales catégories de réseaux mobiles. Un réseau mobile Ad hoc est un système distribué, composé de plusieurs entités autonomes capables de communiquer entre elles via des fréquences radio et peuvent s'auto-organiser et coopérer pour fournir des services.

Les réseaux mobiles Ad hoc ont été initialement développés pour des applications militaires et celles des secours en cas de catastrophes mais leurs propriétés en font des solutions pratiques dans de nombreux domaines de la vie courante et plusieurs applications des réseaux Ad hoc ont vu le jour. Nous citons les réseaux véhiculaires résultant de l'interconnexion de véhicules en mouvement ou les réseaux de capteurs capable de récolter et de transmettre les données environnementales. D'autres situations de la vie courante sont adaptées à l'utilisation des réseaux Ad hoc. C'est le cas par exemple du réseau créé entre un professeur et ses étudiants pour le besoin d'une séance de cours ou le réseau créé entre les participants à une réunion ou même entre les voyageurs dans un train.

Le routage est une fonction primordiale dans les MANET où chaque entité mobile joue le rôle d'un routeur et participe activement dans la transmission des paquets de données. Les nœuds mobiles qui sont dans la même portée radio peuvent communiquer entre eux directement par des liens sans fil tandis que les nœuds qui sont lointains dépendent d'autres nœuds comme routeurs, pour communiquer. Chaque entité dans le réseau compte sur la coopération des voisins pour relayer ses messages. Cette équivalence entre les entités fait que les schémas classiques de routage utilisés dans les réseaux filaires ne s'appliquent plus pour les réseaux Ad hoc, qui nécessitent donc la mise en place de protocoles de routage spécifiques. Ces protocoles de routage Ad hoc spécifient la manière avec laquelle les entités communiquent pour échanger des informations sur la topologie leur permettant de construire leur propre vision du réseau. Il existe trois catégories de protocoles de routage Ad hoc, proactifs, réactifs et hybrides qui se différencient par le mode de fonctionnement de la phase de découverte du chemin et de la mise à jour d'informations de routage.

L'élargissement du domaine d'application des réseaux mobiles Ad hoc nécessite plus de sécurité pour assurer l'intégrité et la confidentialité des données qui circulent dans le réseau. Cependant les protocoles de routage Ad hoc tel que conçus manquent de contrôles de sécurité. La plupart font l'hypothèse d'un comportement honnête entre les entités qui collaborent. La réalité peut toutefois être très différente en présence d'entités malveillantes capables de corrompre le bon déroulement des opérations pour servir leur intérêt. En effet, les réseaux mobiles Ad hoc sont confrontés à de nombreux problèmes liés à leurs caractéristiques qui rendent les solutions de sécurité développées pour les réseaux filaires ou sans fil avec infrastructure inapplicables dans le contexte des réseaux mobiles Ad hoc.

L'absence d'une unité centralisée accentue le défi pour proposer une solution de sécurité comme c'est le cas dans les réseaux filaires ou sans fil avec infrastructure fixe. La mobilité peut causer l'instabilité des chemins parce que les nœuds de ces réseaux peuvent se déplacer de manière imprévisible à des vitesses quelconques comme ils peuvent apparaître et disparaître rapidement. Cette caractéristique nécessite le développement de protocoles de routage sophistiqués et de solutions de sécurité adaptées à un tel environnement, ce qui constitue un vrai défi. Le support de transmission est très vulnérable aux écoutes clandestines. N'importe qui peut joindre le réseau, ainsi il est capable de capturer le trafic, de l'analyser et même d'injecter du nouveau trafic et, de façon générale, ne respecte pas les protocoles utilisés. Les nœuds ne sont pas physiquement protégés, ils peuvent être capturés par des attaquants (l'ennemi), ce qui pose problème au niveau des relations de confiance entre les

nœuds. Ainsi, n'importe quel modèle de sécurité dédié au réseau mobile Ad hoc doit prendre en compte la compromission des nœuds, ainsi que la résistance à cette attaque. Les nœuds mobiles dans les réseaux mobiles Ad-hoc ont des ressources très limitées, comme la capacité de calcul, de stockage et surtout d'énergie. La batterie ne tient pas longtemps si le nœud travaille sans arrêt, ce qui complique davantage le problème de la sécurité.

Pour remédier à ces vulnérabilités, de nombreuses propositions ont été faites en vue d'assurer la sécurité des protocoles de routage dans les réseaux Ad hoc. La plupart des solutions de sécurité sont basées sur la cryptographie établies à l'avance pour assurer la distinction entre les entités qui sont autorisées à prendre part au réseau et les entités qui n'y sont pas autorisées et qui sont considérées comme étant des attaquants. Cependant, ces solutions ne respectent pas les caractéristiques des réseaux mobiles Ad hoc, elles adoptent souvent un schéma centralisé déconseillé dans les réseaux mobiles Ad hoc qui peut aussi devenir un point de vulnérabilité dans ce réseau. En plus, elles sont gourmandes en terme de ressources (capacité de calcul, consommation d'énergie et mémoire de stockage) qui sont très limitées dans les réseaux mobiles Ad hoc. Ces mécanismes de défense adaptés surtout pour défendre contre des menaces externes. Cependant, elles restent inefficaces contre des attaques à partir des nœuds compromis qui se comportent malhonnêtement.

Un nœud malicieux peut potentiellement empêcher la communication entre les nœuds en refusant de les relier. Il agit ainsi dans le but soit de préserver sa propre énergie (égoïsme), soit juste pour interrompre la communication entre les nœuds. De ce fait, de nombreux travaux focalisent sur la détection des comportements du participants de réseaux ont été proposées. Malheureusement ces solutions concentrent sur les attaques actives en négligeant les comportements égoïstes qui peuvent avoir des conséquences dramatiques dans un réseau Ad hoc, ou bien concentrent sur le second type de comportement en négligeant le premier.

Au-delà de ces approches traditionnelles utilisant les techniques cryptographiques classiques et les systèmes de détection d'intrusion, des nouvelles mécanismes développées autour des concepts de communautés de plus en plus proches des modèles sociaux comme la confiance, la réputation, ou la recommandation ont été proposés afin de créer et de gérer la confiance entre les entités actives d'un réseau. Ces solutions opèrent comme des systèmes de détection d'intrusions contre des attaquants internes. En effet, les systèmes de confiance et de réputation permettent, à chaque entité participant à un protocole donné, de mesurer la fiabilité d'une autre entité avant de décider d'interagir ou d'entrer en communication avec elle. Ils

représentent donc un moyen d'inciter ces entités à un bon comportement et à toujours offrir des services ou des ressources de qualité. Les systèmes de réputation sont généralement utilisés pour détecter les entités égoïstes et les forcer à coopérer. Cependant, une entité malhonnête peut avoir une bonne réputation puisqu'elle participe aux opérations du réseau, tout en se comportant mal car elle diffuse de fausses informations. Les solutions à base de systèmes de gestion de confiance usent des propriétés intrinsèques des protocoles de routage pour chercher des incohérences entre les messages reçus. En effet beaucoup de ces solutions ne répondent que partiellement aux exigences de sécurité imposées par la nature des réseaux Ad hoc.

Notre contribution dans ce mémoire consiste à proposer une architecture pour renforcer la sécurité contre les attaques actives et répond aux besoins spécifiques du routage Ad hoc. Cette architecture est distribuée, basée sur un modèle de confiance développé entre les entités pour construire un raisonnement sur le comportement des entités voisines. Elle exige la coopération entre les nœuds, et permet de détecter les comportements malhonnêtes.

Ce modèle de confiance nécessite un mécanisme de surveillance avancé. C'est pourquoi, nous proposons un mécanisme de surveillance sophistiqué, fondé sur l'écoute de voisinage commun entretenir le modèle de confiance pour renforcer la sécurité dans le réseau et détecter la malhonnêteté ainsi que les attaques sur les paquets transmis dans une zone de voisinage. Ceci s'effectuer par un contrôle des messages échangés au niveau de cette zone et des incohérences dans les ouvertures de routes.

Nous choisissons d'appliquer cette approche sur le protocole réactif AODV (Ad hoc on demand Distance Vector). Nous avons présenté une implémentation et évaluation de cette architecture via des simulations, les résultats obtenus prouvent la pertinence du raisonnement sans pour autant influencer les performances du protocole. Cependant notre proposition n'est pas appropriée dans toutes les situations d'usage et pose encore plus de questions.

Ce mémoire est divisé en quatre chapitres et organisé de la manière suivante :

Chapitre 1 : Consacré principalement à l'état de l'art sur les réseaux mobiles Ad hoc. Tout d'abord, nous présentons Les réseaux mobiles sans fil qui peuvent être catégorisés en deux classes : les réseaux avec infrastructure qui utilisent généralement le modèle de la communication cellulaire, et les réseaux sans infrastructure ou les réseaux Ad hoc. Ensuite, nous passons par définitions des réseaux mobiles Ad hoc(MANET), leurs caractéristiques,

leurs domaines d'application. Ensuite, nous présentons les défis dans le MANET qui font l'objet de notre étude.

Chapitre 2 : Après définition du routage qui constitue une fonction principale dans les réseaux Ad hoc, nous présentons les concepts fondamentaux des protocoles de routage Ad hoc notamment à travers la présentation d'exemples de protocoles dans les différentes familles (proactifs, réactifs et hybrides). De plus, nous présentons les différentes architectures et algorithmes à suivre pour les protocoles de routage dans les réseaux Ad hoc.

Chapitre 3 : Consacré à l'état de l'art sur la sécurité dans les réseaux mobiles Ad hoc. Tout d'abord, nous décrivons les différentes vulnérabilités et la classification des attaques dont les réseaux mobiles Ad hoc souffrent. Puis, nous étudions les différentes approches de sécurité dédiées à l'environnement des réseaux mobiles Ad hoc.

Chapitre 4 : Présente notre contribution. Au début nous présentons la notion de confiance et de réputation sur la quelle se base notre architecture. Ensuite nous nous intéressons particulièrement au protocole de routage Ad hoc AODV sur le quel on va faire des améliorations. Puis nous étudions les vulnérabilités d'AODV sur lesquelles des entités malhonnêtes se basent pour mettre en place leurs attaques. Ensuite nous décrivons en détail notre contribution. Après avoir défini l'environnement de simulation, nous présentons l'implémentation de cette solution ainsi que les résultats obtenus après simulations. Enfin, et avant de conclure, nous discutons et commentons les résultats obtenus par simulations.

Chapitre 1. Réseau Ad hoc : principe et caractéristique

1.1. Introduction

Dans le domaine des réseaux de communication, les besoins de mobilité et de pouvoir partager ou échanger l'information à tout moment, en utilisant des dispositifs mobiles (téléphones portables, PDA, PC portables, etc.…) a rendu très répandu la notion de réseau mobile sans fil. Ces réseaux sans fil connaissent aujourd'hui un grand succès grâce à leur grande flexibilité, ils permettent la mise en réseau des sites dont le câblage serait trop onéreux à réaliser dans leur totalité, voire même impossible.

Parmi ces systèmes, les réseaux sans fil avec infrastructure (ou bien cellulaires) connaissent une très forte expansion à l'heure actuelle et ils sont très utilisés dans les réseaux informatiques. Le réseau GSM est un exemple de ce modèle des réseaux sans fil, cependant ce dernier requière une importante infrastructure logistique et matérielle fixe.

Avoir la capacité de satisfaire une communication mobile de nature temporaire, ceci sans aucune infrastructure bien définie a favorisé l'apparition de réseaux mobiles sans infrastructure appelés réseaux Ad hoc. Ce sont la contrepartie des réseaux cellulaires, ils sont formés spontanément à partir d'un ensemble hétérogène de nœuds mobiles (ordinateurs portables, assistants personnels) où la tâche de routage est assurée par les terminaux eux-mêmes pour communiquer entre eux.

Nous commencerons dans ce chapitre par présentation des différents types de réseaux mobiles sans fil dans (section 2), qui explique la différence entre les réseaux sans fil avec infrastructure et les réseaux Ad hoc. Les réseaux Ad hoc ont une architecture de graphe arbitraire dans laquelle, un ensemble de nœuds sans fil forment temporairement un réseau sans l'aide d'une infrastructure ou d'une administration centralisée, nous allons montrer cette architecture dans la troisième section. Mais avant cela nous allons premièrement donner dans cette même section une définition plus précise, fournie par l'IETF, des réseaux MANETs. Ensuite on va expliquer les principales caractéristiques et spécificités des réseaux mobiles Ad hoc: une topologie dynamique, l'absence d'infrastructure, des sources d'énergie limitées... Ces propriétés qui les rendent plus distinctifs, expliquent des faiblesses pouvant fragiliser les réseaux Ad hoc. Elles engendrent de nouvelles problématiques qui n'existaient pas dans les réseaux traditionnels et représentent des défis supplémentaires dans la conception des services

de base du réseau Ad hoc parmi lesquels on va exposer deux défis non négligeables dans les réseaux Ad hoc qui sont le routage et la sécurité sur lesquels notre mémoire se focalise et afin de mettre la lumière sur ces défis, on va les présenter dans les chapitres qui se suivent. La dernière section de ce chapitre sera consacrée à une conclusion de ce chapitre.

1.2. Les réseaux sans fils mobiles

Un réseau mobile est un système composé de sites mobiles, permet à ses utilisateurs d'accéder à l'information indépendamment de leurs positions géographiques. La topologie d'un réseau sans fil mobile est très différente de celle d'un réseau local traditionnel et la connectivité est limitée par la portée radio. En générale les réseaux sans fil et mobiles, peuvent être classés en deux classes : les réseaux mobiles avec infrastructure et les réseaux mobiles sans infrastructure.

1.2.1. Les réseaux mobiles avec infrastructure

Les réseaux sans fil avec infrastructure sont également appelés réseaux cellulaires; Ces réseaux se composent de deux types de terminaux : les terminaux mobiles ou nœuds mobiles qui peuvent se déplacer tout en communiquant via les stations de base ou points d'accès qui sont fixes **[1]**. Les terminaux mobiles se déplacent librement mais ne communiquent jamais directement les uns avec les autres **[2]**. Toutes les communications se font systématiquement vers le point d'accès le plus proche qui se charge ensuite de les relayer à la destination. Pendant que le nœud sort de la gamme d'une station de base, il entre dans la gamme d'une autre station de base. Généralement un réseau d'infrastructure, bâti à partir d'un ou plusieurs « points d'accès » fait le lien entre l'accès sans fil et l'infrastructure de réseau filaire. La Figure1 donnée ci-dessous, dépeint le réseau sans fil avec infrastructure.

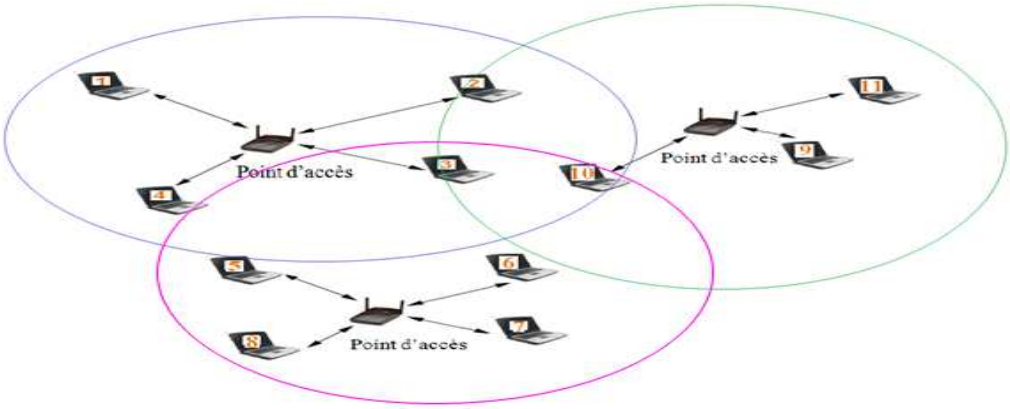

Figure 1.1: Les réseaux mobiles avec infrastructure.

1.2.2. Les réseaux mobiles sans infrastructure

Dans un réseau sans fil sans Infrastructure nommé souvent «peer to peer ou Ad hoc », un nœud mobile peut se déplacer tout en communiquant directement (point à point), il n'y a aucune station de base fixe et la mobilité des nœuds cause des changements fréquents de la topologie du réseau **[3]**. Les nœuds mobiles qui sont dans la portée radio peuvent communiquer entre eux directement par des liens sans fil tandis que les nœuds qui sont lointains dépendent d'autres nœuds comme routeurs, pour communiquer (voir la figure1.2).

La communication sans fil sans Infrastructure est une technologie puissante permettant une connectivité auto-organisée et offre des services de réseau sans aucune infrastructure préexistante. Cette flexibilité permet aux réseaux d'être déployés où il n'y a aucun endroit pour mettre le câblage ou le coût d'installer une infrastructure est prohibitif **[4]**.

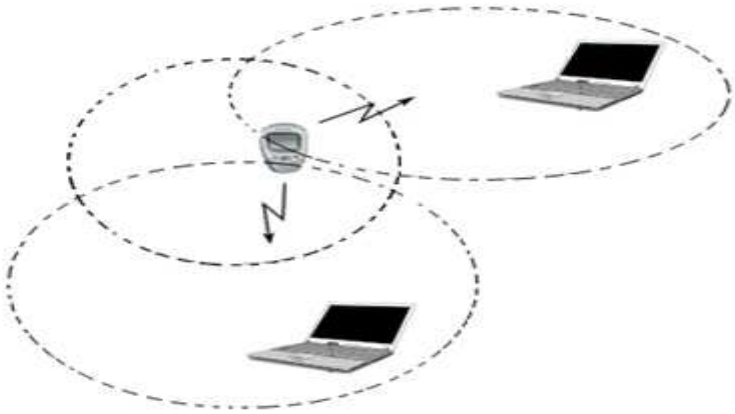

Figure 1.2. Les réseaux mobiles sans infrastructure (Ad hoc).

1.3. Les réseaux mobiles Ad hoc (MANETs)

1.3.1. Définition

Contrairement aux réseaux cellulaires qui sont organisés autour de points d'accès jouant le rôle de routeurs, les réseaux Ad hoc sont des réseaux distribués et spontanés se composant uniquement de terminaux mobiles.

Le groupe MANET (Mobile Ad hoc NETwork) de l'IETF fournit une définition plus précise en introduction de la RFC 2501**[5]***: « Un réseau Ad hoc comprend des plates-formes mobiles (par exemple, un routeur interconnectant différents hôtes et équipements sans fil) appelées nœuds qui sont libres de se déplacer sans contrainte. Un réseau Ad hoc est donc un système autonome de nœuds mobiles. Ce système peut fonctionner d'une manière isolée ou*

s'interfacer à des réseaux fixes au travers des passerelles. Dans ce dernier cas, un réseau Ad hoc est un réseau d'extrémité. »

- Les réseaux mobiles Ad hoc ou MANET (Mobile Ad hoc NETwork) sont constitués de terminaux mobiles équipés de cartes d'interface radio et des couches protocolaires adéquates pour communiquer entre eux et former dynamiquement un réseau mobile; Les nœuds de ces réseaux **[6]** peuvent se déplacer de manière imprévisible à des vitesses quelconques ou ils peuvent apparaître et disparaître rapidement; Cette mobilité peut causer l'instabilité des chemins en les modifiant sans cesse.
- Les nœuds interagissent et peuvent coopérer pour s'échanger des services et la particularité de ce type de réseau mobiles Ad hoc ou MANET (Mobile Ad hoc NETwork) est que chaque nœud peut communiquer avec n'importe quel autre nœud du réseau **[7]**. Un nœud peut à la fois communiquer directement avec d'autres nœuds ou servir de relais, un relais permet à des nœuds se trouvant hors de portée radio les uns des autres de communiquer, un nœud Ad hoc joue donc à la fois le rôle d'un terminal et d'un routeur.

Les réseaux Ad-Hoc font l'objet d'un grand intérêt, ce sont un des éléments moteurs de la recherche dans les réseaux sans fil car leurs domaines d'application sont très nombreux. Les réseaux Ad hoc sont idéals pour les applications caractérisées par une absence (ou la non fiabilité) d'une infrastructure préexistante, ils peuvent utilisés dans des scénarios à des fins militaires, des opérations de secours lors de catastrophes naturelles, ou encore dans des réseaux de capteurs qui sont aujourd'hui avancés.

1.3.2. Modélisation d'un réseau Ad hoc

Un réseau Ad hoc peut être modélisé par un graphe G = (V;E) **[8]** où :

V représente l'ensemble des nœuds (i.e. les unités ou les hôtes mobiles) du réseau et

E modélise l'ensemble des connections qui existent entre ces nœuds.

Si e = (u, v) $\in E_t$, cela veut dire que les nœuds u et v sont en mesure de communiquer directement à l'instant t.

La figure suivante représente un réseau Ad hoc de 10 unités mobiles sous forme d'un graphe :

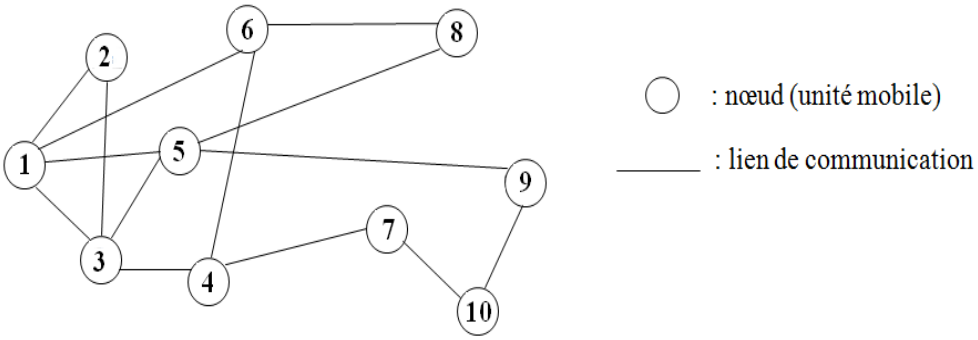

Figure 1.3. La modélisation d'un réseau Ad hoc.

1.3.3. Caractéristiques et contraintes des réseaux mobiles Ad hoc

Un réseau mobile Ad hoc (MANET) est un regroupement de nœuds mobiles formant un réseau temporaire, il intègre des caractéristiques spécifiques entre autres:

1.3.3.1. Communication sans fil

En comparaison de la communication de câble, dans la communication sans fil, les nœuds mobiles utilisent une interface sans fil pour communiquer où les ondes électromagnétiques propagent en air libre et par conséquent des aspects émergeants tel que le trafic par trajets multiples, l'atténuation du signal, le bruit et l'interférence sur le canal, font au canal radio un milieu hostile avec capacité basse, probabilité de collision élevée, et un taux d'erreurs élevé sur les bits **[9]**.

1.3.3.2. L'absence d'infrastructure

Les réseaux Ad hoc se distinguent des autres réseaux mobiles par la propriété d'absence d'infrastructure préexistante et de tout genre d'administration centralisée, il n'y a pas de distinction nette entre les nœuds terminaux (stations, hôtes) qui supportent les applications et les nœuds internes (routeurs, par exemple) en charge de l'acheminement des données. Tous les nœuds peuvent être amenés à assurer des fonctions de routage **[10]**.

Cette caractéristique est fondamentale car elle définit la manière dont les unités mobiles communiquent entre elles et l'organisation du réseau doit donc être distribuée à tous les nœuds, où ils doivent agir en coopération pour manipuler des fonctions de réseau. C'est aussi cette caractéristique qui donne au réseau Ad hoc son extensibilité et sa facilité de déploiement et c'est elle qui rapporte quelques autres propriétés spéciales des réseaux Ad hoc tels que le changement fréquent de topologie et les ressources limitées.

1.3.3.3. Hétérogénéité des nœuds et ressources limitées

Les nœuds Ad hoc peuvent correspondre à une multitude d'équipements (de l'ordinateur portable au capteur intelligent en passant par le téléphone mobile), comme ils peuvent avoir des ressources limitées tel que l'énergie, la capacité de traitement, et la mémoire **[11]**. Ces équipements ne disposent pas des mêmes propriétés physiques et logicielles, mais elles doivent pourtant s'interconnecter facilement pour établir un réseau commun.

1.3.3.4. Des contraintes d'énergie

La consommation d'énergie constitue un problème important pour des équipements fonctionnant grâce à une alimentation électrique autonome. Leurs capacités sont limitées en termes de puissance de calcul, de mémoire, d'énergie (batterie), etc.

Les nœuds dans un MANET fonctionnent souvent avec des batteries et utilisent leurs énergies, en plus de leurs besoins propres, pour router des paquets destinés à d'autres nœuds du réseau **[12]**; cependant les batteries sont difficilement rechargeables en cours de déploiement; pour prolonger la vie du réseau il est alors nécessaire de chercher à réduire la consommation d'énergie ainsi, dans le but de conserver le plus d'énergie possible, les nœuds du réseau ajustent dynamiquement la puissance de leur transmission en fonction de la distance à parcourir et du bruit environnant.

1.3.3.5. Une bande passante limitée

Une des caractéristiques primordiales des réseaux basés sur la communication sans fil est l'utilisation d'un médium de communication partagé **[13]**; Malgré des progrès très importants, Il est difficile de penser pouvoir atteindre sur un médium radio des performances comparables à celles atteintes sur un lien filaire direct et isolé.

La bande passante est moins importante, elle doit être partagée entre les nœuds d'un même voisinage, alors que le routage et la gestion de la mobilité génèrent davantage de flux de contrôle et de signalisation **[10]**. Ces flux doivent être traités de façon prioritaire pour prendre en compte rapidement les modifications de topologie ainsi, la bande passante disponible dépend à la fois du nombre de nœuds présents dans le voisinage et du trafic de données à transporter, indépendamment des perturbations physiques qui peuvent intervenir.

1.3.3.6. Topologies dynamiques et mobilité

Un nœud Ad hoc est libre pour se déplacer arbitrairement, il est susceptible de quitter ou de rejoindre le réseau à tout instant **[13]** car le concept des réseaux mobiles Ad hoc permet d'étendre les notions de la mobilité à toutes les composantes de l'environnement, cette mobilité génère des changements de connectivité, ainsi, la topologie de réseau peut changer aléatoirement et rapidement aux temps imprévisibles, et les techniques de routage classiques, basées sur des routes préétablies, ne peuvent plus fonctionner correctement.

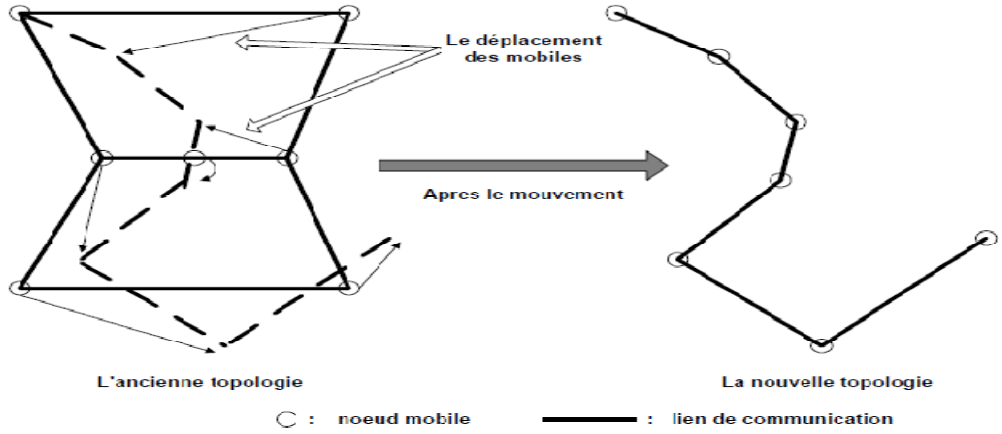

Figure 1.4. Changement de topologie d'un réseau Ad hoc **[14].**

1.3.3.7. La notion de multi-sauts "multihoping"

Dans le modèle cellulaire, la communication entre deux nœuds est faite en utilisant les stations de base et le réseau filaire, par conséquent aucune unité mobile n'est utilisée comme routeur intermédiaire, le modèle cellulaire est dit alors "single hop" (i.e. le nombre de routeurs mobiles intermédiaires est nul). Par contre dans le modèle de communication sans infrastructure ; plusieurs nœuds peuvent participer au routage c'est pour cela l'environnement des réseaux Ad hoc est dit "multi-hop" (i.e. le nombre de stations mobiles qui peuvent être utilisée comme routeurs intermédiaires peut dépasser le un). Il peut donc arriver qu'un nœud mobile veuille communiquer avec un autre qui n'est pas dans sa portée de communication directe ; Les messages vont devoir être transmis de proche en proche jusqu'à la destination.

Cette technique de routage multi-sauts (multi-hops) est illustrée dans **[15]** avec un réseau constitué de quatre nœuds par l'exemple suivant (Figure 1.5) :

Le nœud A envoie directement un paquet à B sans besoin de routage puisque B est dans la portée de communication de A (envoi direct). D'ailleurs, si le nœud A veut envoyer un paquet

au nœud D, il doit utiliser les « services » des nœuds intermédiaires B et C puisque le nœud D n'est pas dans la portée de A.

A envoie le paquet à B ; B transmet le paquet à C ; C, à son tour, transmet le paquet au nœud D.

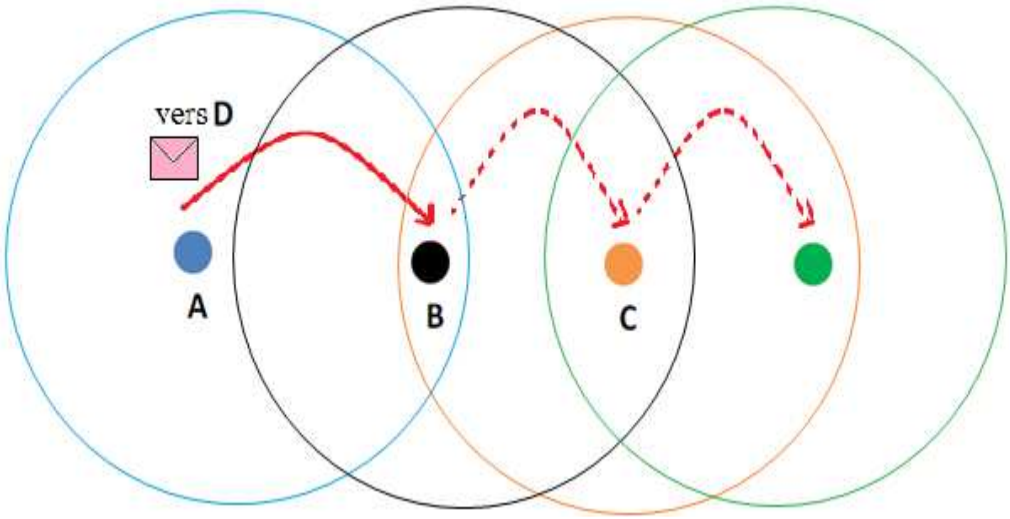

Figure 1.5. Communication multi-sauts entre A et D.

1.3.3.8. Liens asymétriques

Les nœuds peuvent avoir plusieurs interfaces radios, présentant des propriétés de débit ou de fréquences différentes. Ainsi des liens asymétriques (la route inverse n'est pas forcément la même que la route directe) peuvent se créer lorsqu'un élément muni d'un récepteur particulièrement sensible est capable de capter les émissions d'un autre nœud qui est hors de portée du premier élément (voir la figure 1.6 **[16]**) **[7]**. Mais en théorie, les liens sont symétriques car on a un affaiblissement du signal inversement proportionnel à la distance entre l'émetteur et le récepteur.

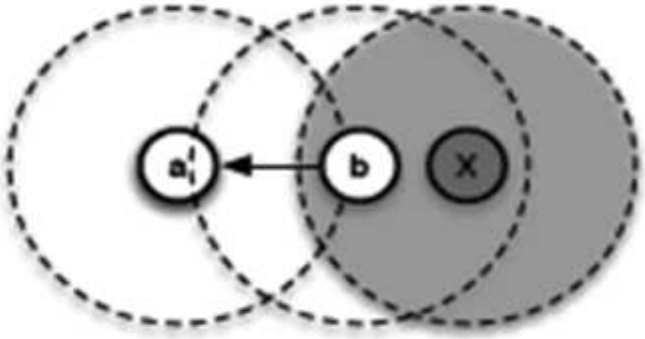

Figure 1.6. Lien asymétrique due à l'interférence radio **[16]**.

1.3.4. Les challenges dans les réseaux Ad hoc

Les réseaux Ad hoc sont promis à un large spectre d'utilisation grâce à ces caractéristiques attrayantes, tout en offrant un système d'échange de données très utile, permettant à un ensemble de nœuds de communiquer, ainsi, chaque station est apte à établir une communication avec n'importe quelle autre station. Toutefois, les réseaux Ad hoc, en plein essor, soulèvent de nombreuses questions, du fait de ces caractéristiques **[17]**, concernant notamment le routage, la conservation d'énergie, la sécurité, la qualité de service...

Afin d'assurer le fonctionnement des réseaux Ad hoc, les nœuds se complaisent dans une relation de confiance avec leurs voisins afin d'acheminer le trafic, saut par saut, d'une source vers une destination mais le trafic peut être détourné de sa destination réelle sans que la source n'en prenne conscience. Pour cela le routage et la sécurité ont fait, et font toujours, l'objet de nombreuses recherches, mais malgré le nombre important des travaux déjà réalisés touchant à plusieurs de ces problématiques inhérentes aux réseaux Ad hoc, les défis faisant face à de tels réseaux, sont encore loin d'être résolus.

1.3.4.1. Le routage

Le problème de routage, en particulier, a suscité un vif intérêt dans la communauté des chercheurs, car les caractéristiques des réseaux Ad hoc posent beaucoup de nouveaux défis en comparaison avec les réseaux câblés traditionnels. Les protocoles existants ne sont pas adaptés aux réseaux Ad hoc, ainsi, de nombreuses solutions utilisant des méthodes variées ont été proposées et étudiées récemment. Bien que les protocoles proposés présentent certaines caractéristiques, ils présentent aussi certaines limites, surtout à forte mobilité des nœuds ou à forte charge du réseau **[18]**. Les différents protocoles ne sont encore que des drafts et restent en cours de développement et de spécification.

Contrairement aux réseaux filaires, une rupture de route ne peut pas être considérée comme un événement rare dans un réseau Ad hoc. En effet, comme chaque nœud doit servir de routeur à ses voisins ; du fait de la mobilité des nœuds, des problèmes de propagation et d'énergie, la topologie d'un réseau Ad-Hoc évolue beaucoup au cours du temps si bien que les routes permettant aux nœuds de communiquer ne sont pas statiques. Dans certains cas, cette mobilité et ces aspects énergétiques peuvent également entrainer des partitionnements du réseau **[2]**. En effet, l'absence d'infrastructure ou d'administration fixes dans le réseau impose

par ailleurs un fonctionnement distribué ; le déplacement des unités mobiles peut remettre en cause la validité des informations de routage. L'algorithme d'obtention d'une route dans un réseau Ad hoc doivent alors tenir compte des caractéristiques particulières de ces réseaux, doit être optimal en terme de rapidité, doit prendre en compte la mobilité des nœuds et doit rechercher la route la plus courte en nombre de sauts.

1.3.4.2. La sécurité

À la différence des réseaux de câble, les réseaux sans fil sont par nature plus sensibles aux problèmes de sécurité **[10]**. les caractéristiques uniques des réseaux Ad hoc mobiles telle que l'architecture ouverte de réseau (Peer-to-Peer), le milieu sans fil partagé, les contraintes rigoureuses de ressource, et la topologie de réseau fortement dynamique, lancent un certain nombre de défis non triviaux à la conception de sécurité. Mais pour les réseaux Ad hoc, le principal problème réside dans le fait que tous les nœuds sont équivalents et potentiellement nécessaires au fonctionnement du réseau. Un nœud n'a pas forcément de connaissance à priori sur les autres, la confiance n'est donc pas aussi simple que dans le cas des réseaux classiques, la détection d'une intrusion ou d'un déni de service est plus délicate, et l'absence de centralisation engendre des faiblesses **[19]** et pose un problème de remontée de l'information de détection.

Les réseaux sans fil Ad hoc sont vulnérables à plusieurs attaques **[20]**. Les possibilités de s'insérer dans le réseau sont plus grandes et dans la plupart des cas, un attaquant peut facilement injecter les paquets faux, personnifiant un autre expéditeur. Un attaquant peut également perturber l'opération d'acheminement, il peut facilement écouter clandestinement la communication, enregistre les paquets, et rejoue les paquets. Afin de fournir la communication protégée entre les nœuds mobiles dans un environnement hostile, la sécurité est devenue un souci primaire **[21]** et de nombreux efforts sont mis en œuvre pour trouver des solutions au problème de sécurité.

1.4. Conclusion

Nous avons présenté dans ce chapitre les concepts de base des réseaux Ad hoc en faisant ressortir leurs propriétés les plus importantes à savoir l'absence d'infrastructure, l'auto-organisation et le type du medium de communication. Dans les MANETs chaque entité mobile joue le rôle d'un routeur et participe activement dans la transmission des paquets de données. Ainsi, une entité peut communiquer directement avec une autre si elle est dans sa

portée radio. Sinon, elle compte sur la coopération des voisins pour relayer ses messages. Nous avons vu aussi que, étant donné les spécificités des réseaux Ad hoc, notamment, l'absence d'infrastructure, l'utilisation de liens sans fil et les changements fréquents de topologie. Les solutions proposées tant au niveau routage d'un réseau informatique en général ne sont pas réutilisables telles qu'elles dans les réseaux Ad hoc. Celles-ci nécessitent en effet une réadaptation aux caractéristiques intrinsèques du réseau Ad hoc.

La nature des réseaux Ad hoc, où les nœuds sont mobiles et peuvent se joindre ou quitter le réseau à tout moment, présente des grands défis pour la sécurité et le routage. Or la sécurité est le point névralgique des réseaux Ad hoc. Il est donc primordial de préserver la confidentialité, l'intégrité, la non répudiation et la disponibilité dans ce type d'environnement. Pour se faire, il est important de prévenir les attaques en particulier contre les protocoles de routage. Or, ces derniers ne proposent pas de modèles de sécurité ou des mécanismes pour faire face aux différents types d'attaques. Il y'a beaucoup de questions de recherche encore ouverte et le routage fait une fonction primordiale dans les MANET comme nous verrons dans le prochain chapitre.

Chapitre 2. Protocole de routage dans les réseaux Ad hoc

2.1. Introduction

Le routage est une méthode d'acheminement des informations vers une destination donnée dans un réseau de communication. Les méthodes de routage traditionnelles sont des méthodes éprouvées, qui fonctionnent parfaitement. Cependant, elles ne sont pas adaptées aux cas de topologies fortement variables. Vu les caractéristiques des réseaux Ad hoc, le routage dans ces réseaux présente de nombreux challenges pour la communauté scientifique et constitue un thème essentiel de recherche. Il faut avant tout trouver un moyen pour router les données dans le réseau de façon efficace, les protocoles de routage doivent donc être distribués, et sans boucle, ils doivent être en mesure d'optimiser les ressources du réseau et empêcher les collisions, il est également indispensable de concevoir un protocole efficace lorsque le nombre de participants et leur mobilité augmentent, un protocole de routage Ad hoc doit s'adapter rapidement aux changements relativement fréquents dans la topologie, il doit être optimal en terme de rapidité et doit rechercher la route la plus courte en nombre de sauts.

Le routage dans les réseaux mobiles Ad hoc a alors été très étudié ces dernières années, et ceci s'est traduit par l'apparition de centaines de protocoles dans la littérature, parmi lesquels seulement quelques uns ont été soumis à normalisation par le groupe de travail de l'IETF Mobile Ad hoc Networking (MANET). Les protocoles de routage dédiés aux réseaux Ad hoc peuvent être caractérisés par leur catégorie (protocoles proactifs, réactifs ou hybrides), leur architecture (à plat ou hiérarchique) ainsi que par leur type d'algorithmes.

Dans ce chapitre, nous présentons un état de l'art non exhaustif des principales solutions de routage dans les réseaux ad-hoc, Nous tenterons dans la première partie de mettre une définition de routage qui constitue une fonction principale dans les réseaux Ad hoc. Il s'agit du mécanisme par lequel les chemins sont créés, et des règles qui spécifient la manière avec laquelle les entités communiquent entre eux pour échanger des informations sur la topologie leur permettant de construire leur propre vision du réseau, dans la deuxième section alors on va parler des différentes architectures pour les protocoles de routage dans les réseaux Ad hoc qui sont notamment les protocoles de routage « à plat » et les protocoles de routage hiérarchique. Dans la troisième section on va donner les principaux algorithmes à suivre dans le routage Ad hoc, qui sont : l'inondation, le vecteur de distance, l'état de lien.

L'équivalence entre les entités des réseaux dans un processus de routage dont chacune d'elles est un routeur, fait que les schémas classiques de routage utilisés dans les réseaux classiques ne s'appliquent plus pour les réseaux Ad hoc, ceci nécessite la mise en place de protocoles de routage spécifiques. Dans la suite de ce chapitre, nous présentons les différentes familles de protocoles de routage, en basant sur quelques exemples détaillant le fonctionnement de certains de ces protocoles (quatrième section). En effet, il existe trois catégories de protocoles de routage Ad hoc, proactifs, réactifs et hybrides qui se différencient par le mode de fonctionnement de la phase de découverte du chemin et de la mise à jour d'informations de routage. Nous terminerons par une conclusion, en mettant en relief les principaux points discutés dans ce chapitre.

2.2. Le routage dans les réseaux mobiles Ad hoc

Comme nous avons déjà vu dans les sections précédentes, l'architecture d'un réseau mobile Ad hoc est caractérisée par une absence d'infrastructure fixe préexistante, en plus les nœuds peuvent apparaître, se déplacer et disparaître spontanément dans le réseau, par conséquent, aucune information préalable concernant la topologie et l'état du réseau n'est disponible. En outre dans la plupart des cas, l'unité destination ne se trouve pas obligatoirement dans la portée de l'unité source ce qui implique que l'échange des données entre deux nœuds quelconques, doit être effectué par des stations intermédiaires (notion de multi-sauts). Afin de permettre les communications multi-sauts entre des nœuds hors de portée de transmission, une des fonctions fondamentales dans les réseaux Ad hoc est le routage. Il s'agit du mécanisme par lequel les chemins sont créés pour acheminer les données à la bonne destination à travers le réseau. Cette fonction est divisée en deux parties **[22]** : une phase de signalisation assurée par des échanges de messages de contrôle (ou le protocole de routage) et une phase d'acheminement des paquets de données de bout en bout (ou le service de routage).

- Le protocole de routage est un ensemble de règles qui spécifient la manière avec laquelle les routeurs communiquent entre eux pour échanger des informations sur la topologie leur permettant de construire leur propre vision du réseau.
- Le service de routage assure quant à lui la transmission des paquets de données en utilisant la vision construite précédemment.

Nous constatons que ces deux définitions sont complémentaires : sans le protocole de routage, il n'y aurait plus de vision du réseau ce qui empêche l'acheminement des données vers la destination, partie assurée par le service de routage.

2.3. Architecture de routage « hiérarchique ou plat »

Les protocoles de routage dans les réseaux Ad hoc peuvent être classés suivant plusieurs critères. Le premier d'entre eux concerne le type de vision qu'ils ont du réseau et les rôles qu'ils accordent aux différents mobiles.

2.3.1. Les protocoles de routage « à plat » (flat based-routing)

Ces protocoles considèrent que tous les nœuds sont identiques (voir la figure 2.1), c'est à dire ont les mêmes fonctions à exécuter. La décision d'un nœud de router des paquets vers un autre dépendra de sa position et pourra être remise en cause au cours du temps. Parmes les protocoles utilisant cette technique, on cite l'AODV (Ad hoc On Demand Distance Vector).

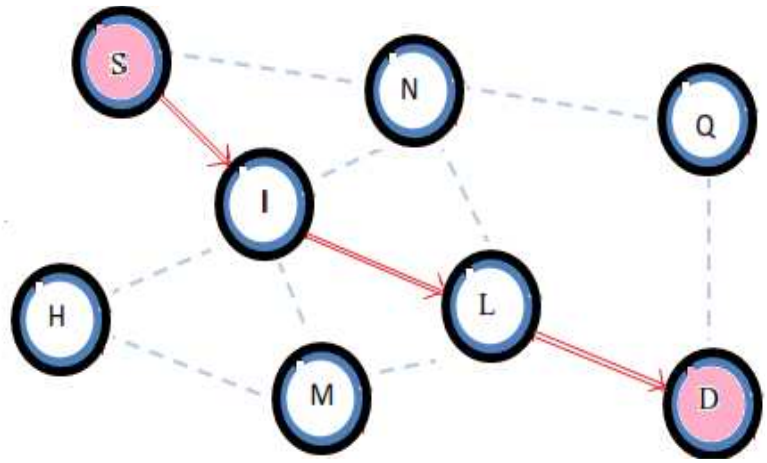

Figure 2.1. Routage « à plat ».

2.3.2. Les protocoles de routage hiérarchique

Ces protocoles fonctionnent en confiant des rôles qui varient de l'un à l'autre. Certains nœuds sont élus et assument des fonctions particulières qui conduisent à lui. Un nœud peut être, par exemple, une passerelle pour un ensemble de nœuds. Dans ce cas, le routage devient plus simple, puisqu'il s'agit de passer par les passerelles pour atteindre le nœud destination qui lui est directement attaché. Dans la figure 2.2 : Pour que les paquets générés par le nœud S atteignent le nœud D, ils doivent passer par les passerelles P, L et R. Un exemple de protocole utilisant cette stratégie est l'OLSR (Optimized Link State Routing).

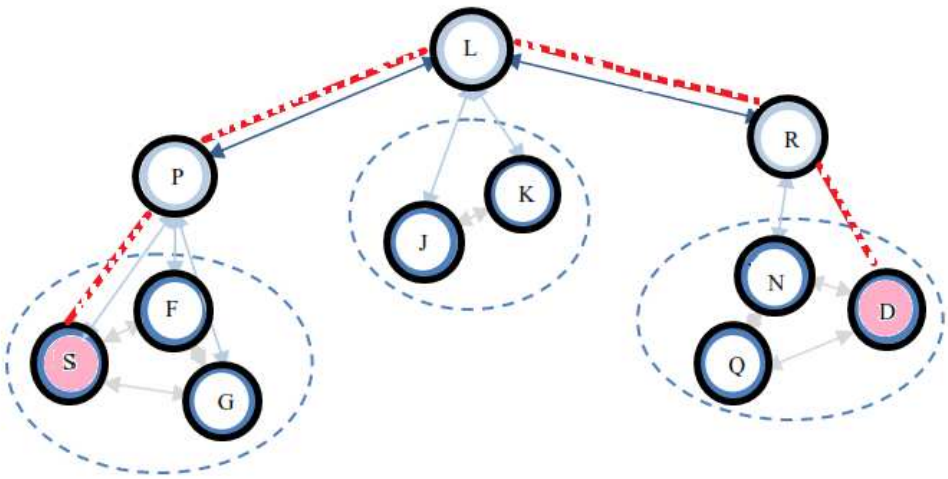

Figure 2.2. Routage hiérarchique.

2.4. Méthodes de routage traditionnel

Les protocoles de routage dans les réseaux Ad hoc sont fondés sur les principes fondamentaux du routage dans les réseaux classiques, qui sont : l'inondation, le vecteur de distance et l'état de lien. Ces algorithmes permettent de déterminer la route que doivent emprunter les messages dans un nœud. Pour cela, ils gèrent les tables de routage de chaque nœud, en veillant notamment à ne pas créer des problèmes durant l'opération d'acheminement des paquets entre les unités en communication.

2.4.1. L'inondation

Dans les protocoles de routage pour les réseaux Ad hoc, l'inondation ou la diffusion pure consiste à propager un paquet (de données ou de contrôle) dans l'ensemble du réseau **[8]**. Un nœud qui initie l'inondation envoie le paquet à tous ses voisins directs. De même, si un nœud quelconque du réseau reçoit le paquet, il le rediffuse à tous ses voisins. Ce comportement se répète jusqu'à ce que le paquet atteigne tous les nœuds du réseau comme illustré dans la figure 2.3.

Notons que les nœuds peuvent être amenés à appliquer, durant l'inondation, des traitements de contrôle, dans le but d'éviter certains problèmes, tels que le bouclage et la duplication des messages **[23]**, par exemple, utiliser un champ de durée de vie (time to live) dans les paquets transmis, ce champ va décrémenter à chaque retransmission du paquet. Lorsque la valeur du champ est nulle, alors le paquet n'est pas retransmis. On peut aussi utiliser une seconde approche, qui peut complémenter la première, consiste à éviter d'envoyer

une seconde fois les paquets déjà retransmis. Chaque paquet doit donc disposer d'un identifiant (adresse de la source couplée avec un numéro de séquence incrémenté à chaque paquet émis par la source) afin de déterminer si le paquet a déjà été reçus et retransmis. Un paquet avec un identifiant connu sera donc ignoré, et il n'y aura pas de duplication inutile des paquets dans le réseau.

Le mécanisme d'inondation est utilisé généralement dans la première phase du routage, plus exactement dans la procédure de découverte de route, et dans le cas où le nœud émetteur ne connait pas la localisation exacte de la destination. La source inonde le réseau avec un paquet de recherche de route afin qu'il atteigne le nœud destinataire. En fait, Le routage par inondation a pour particularité une grande robustesse en raison de la redondance liée à l'inondation. Cependant l'inondation est très couteuse surtout dans le cas ou le réseau est volumineux (latence, surcharge des messages, etc.). C'est pour cela que les protocoles de routage essaient de minimiser au maximum possible la propagation des paquets de découverte de topologie par inondation en ajoutant d'autres paramètres de diffusion.

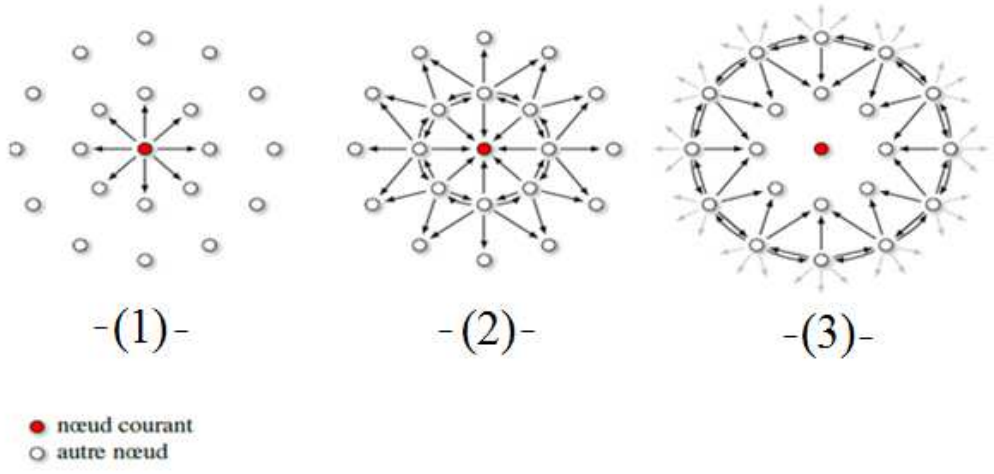

Figure 2.3. Le mécanisme d'inondation.

2.4.2. Le routage par vecteur de distance (Distance Vector (DV))

Les protocoles de routage à vecteur de distance sont conçus pour être exécutés sur de petits réseaux et se basent sur l'algorithme de Bellman-Ford distribué pour calculer le meilleur chemin **[15]**. Plutôt que de maintenir une carte complète du réseau comme nous avons déjà vu avec le routage par inondation, ces protocoles sont orientés destination. Au début, chaque nœud détecte ses voisins directs et construit sa propre table de routage puis il la diffuse à ses voisins. Les tables sont mises à jour en fonction des informations reçues (ajout et modification

d'une entrée) et convergent jusqu'à ce que la structure du réseau à travers ces tables se stabilise. Chaque entrée de la table de routage est un triplet (nœud destinataire, nœud suivant, métrique) où la métrique est le coût de la route pour atteindre le nœud destinataire en passant par le nœud suivant. Généralement, la métrique utilisée pour cet algorithme est le nombre de sauts **[23]**, mais d'autres métriques peuvent être utilisées (comme le délai d'acheminement, le nombre total de paquets en file d'attente pour ce parcours).

Un des problèmes de cette méthode est que l'information d'une rupture de lien se propage très lentement. En outre la construction des tables de routage est réalisée par vagues, de manière distribuée, ce qui peut entraîner des boucles de routage. En raison de ces problèmes et parce qu'il était plus adapté à des réseaux de taille limitée, le routage par vecteur de distance a été assez rapidement abandonné au profit du routage par état de lien **[23]**.

2.4.3. Le routage par état de lien (Link State (LS))

L'algorithme vu précédemment peut présenter des problèmes de convergence c'est-à-dire conduire à des boucles de routage. Pour éviter complètement les boucles il faut que chacun des nœuds ait une connaissance globale de la topologie du réseau. L'objectif de l'algorithme Link State **[24]** est donc de donner aux nœuds cette connaissance. Les messages de contrôle sont diffusés par les nœuds à tout le réseau et contiennent la topologie locale de l'émetteur, c'est-à-dire la liste de ses voisins. On parle alors de messages topologiques. En regroupant les topologies locales de tous les nœuds du réseau, un nœud peut reconstituer la topologie globale et utiliser cette information pour appliquer une méthode de calcul de route appropriée, en générale le calcule du plus court chemin se fait à l'aide de l'algorithme de Dijkstra **[15]**.

Le routage par état de lien a pour avantage de répondre rapidement aux moindres changements sur le réseau en envoyant des mises à jour déclenchées uniquement après qu'une modification soit survenue. Le revers de la médaille est que la diffusion des messages topologiques à tout le réseau ne passe pas bien à l'échelle et donc cette technique a longtemps été négligée par les chercheurs.

2.5. Classification des protocoles de routage

En règle générale, les protocoles de routage s'appuient sur l'échange de messages de contrôle entre les nœuds du réseau pour acquérir les informations nécessaires à leur fonctionnement et suivant la méthode de création et la maintenance des routes lors de

l'acheminement des paquets, les protocoles de routage dans les réseaux Ad hoc peuvent être classés en trois catégories : protocoles proactifs, réactifs et hybrides.

- La première catégorie est celle des protocoles proactifs dans lesquels les nœuds maintiennent des informations topologiques tout au long de leur participation dans le réseau. Ces informations sont utilisées pour disposer à tout moment d'un chemin vers toute destination possible dans le réseau, sans nécessiter d'échange de messages de contrôle supplémentaires lors de l'envoi d'un paquet de données.
- La seconde catégorie est celle des protocoles réactifs qui, contrairement aux protocoles proactifs, ne maintiennent pas d'information topologique a priori. Les routes sont recherchées à la demande, lorsqu'un paquet de données est destiné à un nœud pour lequel aucun chemin n'est connu.
- Pour la dernière catégorie qui est celle des protocoles hybrides, il s'agit essentiellement d'une combinaison des protocoles proactifs et réactifs afin de tirer parti des avantages de chacun d'eux.

La figure 2.4 montre une classification des protocoles de routage dans les réseaux Ad hoc, avec une illustration par les protocoles les plus connus de chacune de ces catégories annoncés auparavant.

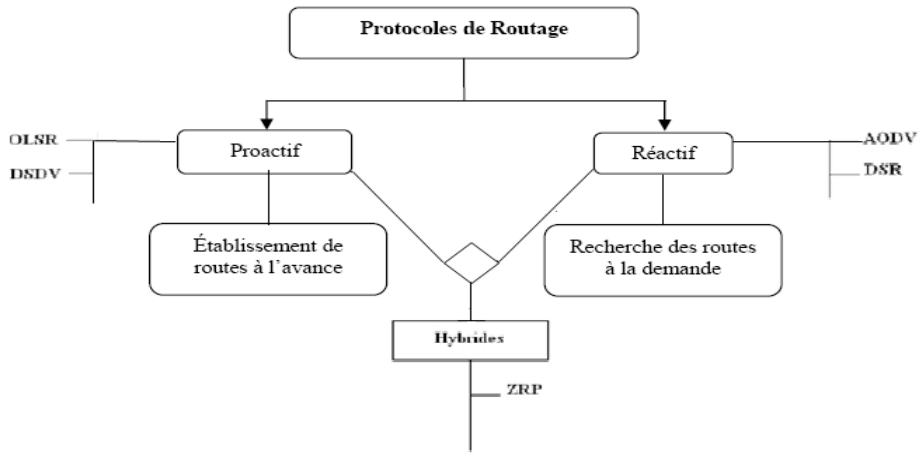

Figure 2.4. Classification des protocoles de routage Ad hoc.

2.5.1. Les protocoles proactifs

Les protocoles de routage proactifs se basent sur l'établissement de routes à l'avance. Les nœuds mettent à jour périodiquement les données de routage de façon à obtenir en permanence le plus court chemin (calculé en terme du nombre de nœuds intermédiaires, aussi appelé nombre de sauts) vers tous les nœuds du réseau. Ainsi, si un nœud désire transmettre

un paquet vers une destination, il consulte sa table de routage qui lui indique immédiatement le chemin à suivre. ce type de protocoles se basent sur deux approches(discutées dans les sections précédentes), l'approche vecteur de distance et l'approche à état des liens qui exigent toutes les deux une mise à jour périodique des données de routage qui doit être diffusée par les différents nœuds de routage du réseau. Chaque nœud mobile, routeur potentiel, construit ou maintient à jour une ou plusieurs tables de routage par l'échange régulier de messages sur la topologie du réseau avant même que la demande en soit effectuée **[1]**, pour accélérer le routage des paquets, cette approche permet alors de disposer d'une route vers chaque destination immédiatement au moment où un paquet doit être envoyé. La propagation des messages de mise à jour de ces tables est effectuée même quand les routes ne sont pas utilisées et même s'il n'y a pas de trafic circulant dans le réseau **[25]**.

L'avantage des protocoles proactifs est que chaque nœud connait à tout moment l'entièreté du réseau et, quand un message doit être envoyé, aucun temps n'est perdu dans une recherche de chemin. Malheureusement ces protocoles atteignent rapidement leurs limites avec l'accroissement du nombre de nœuds et de leur mobilité. Le réseau est continuellement encombré par un trafic de contrôle dont une partie importante est inutile **[2]**, ce qui va augmenter le surcoût d'une part et qu'il va diminuer d'autant la bande passante disponible pour les applications d'une autre part.

Dans ce qui suit, nous détaillons ces approches par l'intermédiaire d'un exemple de protocoles proactifs de routage Ad hoc : DSDV **[26].**

2.5.1.1. Le protocole DSDV (Destination-Sequenced Distance Vector)

DSDV **[26]** (Destination-Sequenced Distance-Vector) est l'un des premiers protocoles mis au point par le groupe MANET **[27]**, **[28]**. Il s'agit d'un protocole orienté destination, basé sur l'algorithme de Bellman-Ford qui a été modifié pour s'adapter aux réseaux Ad hoc. Comme il s'agit d'un protocole proactif, chaque nœud, à chaque instant a une vision complète du réseau, il suppose que tous les nœuds du réseau disséminent une copie de leur vecteur de distance, c'est-à-dire, de leur table de routage, dans laquelle sont entrées toutes les destinations accessibles, ainsi que le nombre de nœuds intermédiaires par lesquels transiter pour atteindre la destination. Les nœuds du réseau maintiennent leurs tables de routage de manière périodique à travers le réseau grâce à des échanges périodiques d'informations sur leurs tables de routage respectives, ce qui génère un trafic important qu'il faille limiter. Pour cela, deux types de paquets de mise à jour sont utilisés **[29]** :

- Les "fulls dump" servent à des mises à jour complètes, contenant toutes les informations, dans ce cas la totalité de la table de routage est envoyée par une station à ses voisins ce qui nécessite l'envoi de plusieurs paquets de données
- Des paquets plus petits qui servent à des mises à jour incrémentales, ne contenant que les informations ayant changé depuis le dernier full dump (c'est-à-dire la dernière mise à jour), dans ce cas juste les entrées qui ont subit un changement par rapport à la dernière mise à jour, sont envoyées ce qui réduit le nombre de paquets transmis.

La façon de faire la mise à jour des tables de routage est liée à la stabilité du réseau. Dans le cas où le réseau serait relativement stable, la mise à jour incrémentale est utilisée pour réduire le trafic de la communication. Dans le cas opposé, où le réseau subit des changements rapides, le nombre de paquets incrémentaux envoyés augmente, ce qui fait que la mise à jour complète est fréquente.

Outre son adresse et son propre numéro de séquence, chaque paquet de mise à jour doit contenir une liste des routes ajoutées/modifiées pour laquelle chaque entrée est un triplet formé par : l'adresse de la destination, le nombre de sauts pour l'atteindre (Hop Count) et le dernier numéro de séquence connu associé à cette destination (Sequence Number) qui permet notamment de distinguer les nouvelles routes des anciennes et évite ainsi la formation de boucles de routage.

Pour gérer la mobilité des nœuds, DSDV associe à chaque nœud un minuteur (timer) qui est mis à jour à la valeur maximale à chaque fois qu'un message est reçu du voisin : c'est un indicateur de validité du lien. Ainsi, lorsque ce minuteur expire, le nœud considère que le voisin en question n'est plus à porté radio et que le lien est rompu. Il peut aussi utiliser les messages de la couche MAC pour détecter les ruptures de liens. La détection d'un lien rompu se traduit au niveau de l'entrée correspondante dans la table de routage. Toutes les routes utilisant ce nœud qui n'est plus joignable sont aussi mises à jour comme étant des routes invalides. Ces changements sont envoyés en priorité à tous les voisins en utilisant un paquet de mise à jour. À la réception d'un paquet de mise à jour, les routes avec les plus grands numéros de séquences sont privilégiées pour le choix des routes puisque cela signifie une route plus fraîche. Dans le cas de numéros de séquences égaux, le plus court chemin est retenu en se basant sur le nombre de saut. Le nœud intermédiaire procède ensuite à la rediffusion des informations qu'il vient de modifier dans sa table de routage tout en incrémentant son numéro de séquence.

Malgré les améliorations qu'il propose grâce notamment à l'utilisation des numéros de séquence, DSDV reste long et coûteux. Il nécessite des mises à jour régulières de ses tables de routage même lorsque le réseau est inactif. À chaque mise à jour, un nouveau numéro de séquence est nécessaire ce qui augmente le temps avant que le réseau converge. Ceci rend DSDV peu adapté aux réseaux très dynamiques.

2.5.2. Protocole réactif

À l'inverse des protocoles proactifs, les protocoles réactifs à la demande n'ont pas une vision complète du réseau, ils ne construisent pas de tables de routage au préalable. SI un nœud a besoin de communiquer avec un autre nœud, seulement à cet instant, il entreprend une recherche de route et lorsque le chemin est établi, l'acheminement des données peut commencer. Un processus de découverte de route est réalisé suivant le principe de requête-réponse **[25]**, un nœud envoie des requêtes de recherche de route et attend en retour une réponse lui indiquant le chemin à suivre, ainsi les routes peuvent ensuite être stockées dans une table de routage locale et être maintenues par l'envoi périodique de messages de signalisation. En effet selon l'approche utilisée pour acheminer les paquets vers leur destination à savoir l'état de lien ou le vecteur de distance les protocoles de routage réactifs se diffèrent d'un protocole à un autre **[30]**. Parmi les protocoles basés sur ce principe on cite : DSR, AODV, TORA, ABR, SSR, LAR, RDMAR, EARP et CEDAR…Nous présentons dans ce qui suit les protocoles DSR **[23]** et AODV **[31]** qui utilisent respectivement l'approche état de lien et l'approche vecteur de distance.

De manière générale, ces protocoles sont utilisés dans des réseaux à forte mobilité **[2]** où les communications entre nœuds sont plus ponctuelles et ne nécessitant pas une connexion permanente avec tous les nœuds du réseau. Le trafic de contrôle requis pour obtenir une route est minimisé car les mécanismes ne sont déployés qu'en cas de besoin. Le surcoût occasionné par la mise à jour des informations de routage est directement proportionné, au cas par cas, aux flux de données circulant dans le réseau, cependant la durée d'obtention d'une route est souvent plus longue que pour un protocole proactif car la recherche d'un chemin vers la destination commence uniquement lorsque la source veut transmettre des données **[25]**.

2.5.2.1. Le protocole de routage DSR (Dynamic Source Routing)

DSR (Dynamic Source Routing) est proposé par Johnson et Maltz **[22]**, il est un des premiers protocoles de routage qui a été proposé pour les réseaux Ad hoc mobile multi sauts **[23]**. C'est un protocole de routage réactif à état de lien, Les routes sont construites à la

demande, cependant ce protocole à la particularité de ne pas nécessiter la présence de tables de routage sur les différents nœuds du réseau, puisqu'il repose comme son nom l'indique sur le principe du routage par la source. Les informations sur les chemins sont réparties entre tous les nœuds, et les messages de contrôle contiennent la liste de tous les nœuds formant les chemins à partir de la source. La figure 2.7 explique le principe de routage par la source: chaque nœud inclut son adresse dans l'entête du paquet de telle sorte qu'en arrivant à la destination, le paquet contient une liste complète et ordonnée de nœuds par lesquels le paquet a transité de la source à la destination (figure 2.7a). Cette liste est renvoyée à la source dans un paquet de réponse de route (figure 2.7b).

Les deux opérations (processus) de base du protocole DSR sont : la découverte de routes (route discovery) et la maintenance de routes (route maintenance). La première opération permet de déterminer automatiquement les routes nécessaires à la communication entre nœuds, tandis que la seconde permet de s'assurer de la correction des routes tout au long de leur utilisation. Nous donnons plus de détails sur ces deux processus dans ce qui suit.

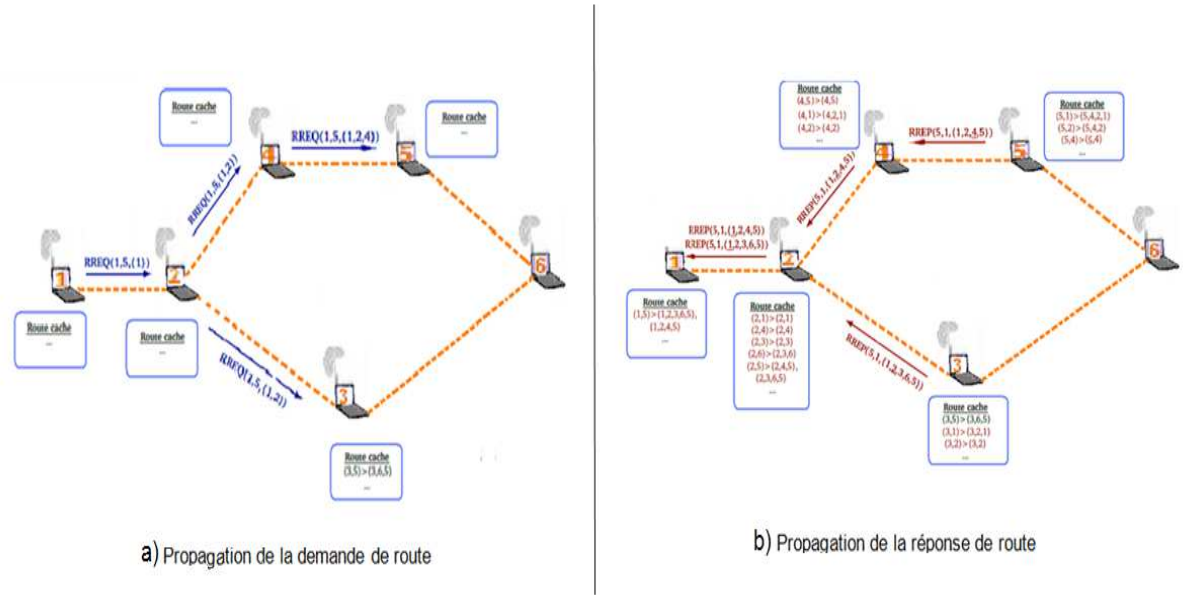

Figure 2.7. Exemple du processus d'établissement de route entre 1 et 5.

a) Le mécanisme de découverte de route (Route Discovery)

Pour trouver une route, lorsqu'un nœud source désire envoyer des données à une destination (le nœud 1 dans la figure 2.7 désire envoyer des données au nœud 5) et qu'il ne trouve pas de route disponible pour cette destination dans son cache (route cache), DSR initie

une demande de route en émettant un paquet en diffusion (broadcast) d'en-tête Route REQuest (RREQ), qui va inonder le réseau comme illustré dans la figure 2.3.

Le paquet RREQ contient un identifiant unique (route request identifier), la destination à atteindre et une liste d'adresses de nœuds (cette liste constituera le chemin entre la source et la destination à la fin du processus de découverte) qui contient initialement uniquement l'adresse de la source (c'est le cas du nœud 1 dans la figure 2.7a). Lorsqu'un nœud intermédiaire entre la source et la destination reçoit la demande de route RREQ, il commence par vérifier s'il ne s'agit pas d'une requête déjà traitée en cherchant dans l'historique l'existence du couple identifiant cette RREQ. Si c'est le cas, le paquet est ignoré sinon, le nœud va concaténer son adresse à la liste contenue dans le RREQ et le diffuser à son tour après l'avoir ajouté dans son historique (C'est le traitement que les nœuds 2 et 4 ont suivi dans l'exemple de la figure 2.7a).

Quand le nœud destinataire (cas du nœud 5 dans la figure 2.7a) reçoit le paquet RREQ où la liste contenue dans le paquet constitue le chemin complet pour l'atteindre, il retourne à la source un paquet d'en-tête Route REPly (RREP) en y copiant la liste contenue dans la RREQ reçue et en insérant son adresse à la fin de cette liste. En outre, dans le réseau, les nœuds peuvent enregistrer dans leur cache des informations de routage obtenues au travers des différents paquets de découverte de route reçus et des paquets de données (la figure 2.7b). De plus, si un nœud intermédiaire qui reçoit un RREQ possède une route qui mène à la destination dans son route cache (cas du nœud 3 dans la figure 2.7a), le nœud intermédiaire, dans cette situation, peut générer une réponse de route (RREP) en concaténant le chemin qu'il a reçu dans le paquet RREQ avec celui qui se trouve dans son route cache.

À la fin du processus de découverte de route, un nœud source peut avoir dans son cache plusieurs routes pour atteindre certaines destinations. Une fois ces routes connues, il devra choisir une route en se basant sur le plus court chemin ou en utilisant une autre métrique, ainsi le chemin est établi entre la source et la destination et la transmission de données peut débuter.

b) Le mécanisme de maintenance de route (Route Maintenance)

Lors de la transmission d'un paquet, chaque nœud est responsable de l'acheminement des données sur le lien en direction du prochain saut. Dans un réseau Ad hoc, les nœuds étant mobiles, il faut vérifier, après l'envoi d'une donnée, que la topologie est toujours la même. Pour ce faire, DSR utilise le mécanisme de Route Maintenance. Lorsqu'un nœud initie ou relaie un paquet de données, il devra s'assurer que le nœud suivant (du prochain saut) dans le

chemin a effectivement reçu le paquet. Un accusé de réception peut garantir la confirmation de la validité du lien, cet accusé peut être un accusé de niveau MAC ou en entendant la retransmission du destinataire, comme il peut être dans le cas échéant un accusé spécifique à DSR **[32]**. En cas d'échec total du Route Maintenance, c'est à dire si un nœud ne reçoit pas un accusé de réception suite à un envoi de paquet, il considère que le lien est rompu et supprime cette route du cache. Il crée alors un paquet erreur de route RERR (Route ERRor) qu'il envoie à tous les nœuds ayant envoyé un paquet sur ce lien depuis le dernier accusé de réception. Dans ce cas, il faudra choisir une nouvelle route ou recommencer une procédure de découverte de route dans le cas échéant.

2.5.2.2. Le protocole de routage AODV (Ad-hoc On Demand Distance Vector)

AODV (Ad hoc On Demand Vector routing) **[31]** est un protocole de routage réactif, développé par la firme Nokia est particulièrement adapté aux réseaux qui affichent une topologie fortement dynamique, il est considéré comme la combinaison de DSR et de DSDV.

AODV est un protocole à vecteur de distance qui s'inspire de DSDV. Contrairement à celui-ci, il est réactif plutôt que proactif car il ne demande une route que lorsqu' il en a besoin. En effet, dans son fonctionnement, il associe les mécanismes réactifs de découverte et de maintenance de routes avec le routage par sauts de DSR, il ne construit pas a priori la table de routage mais réagit à la demande, il utilise une requête de route dans le but de créer un chemin vers une certaine destination et essaie de trouver ce chemin avant de router les informations. Tant que la route reste active entre la source et la destination, le protocole de routage n'intervient pas, ce qui diminue le nombre de paquets de routage échangés entre les nœuds constituant le réseau. La communication et l'échange de messages entre nœuds dans le réseau se fait sur deux mécanismes "Découverte de route" et "Maintenance de route" qui seront décrites ci-dessous.

a) La découverte de route

Le mécanisme de découverte de route est analogue à celui du DSR, c'est le processus de recherche de route à la demande des nœuds sources. Si aucune route n'est disponible (la route peut être non existante, avoir expiré ou être défaillante), une requête de découverte de la route RREQ (Route REQuest) se fait par inondation (Figure 2.3) : Le RREQ (contient un identifiant associé à l'adresse de la source qui servira à identifier de façon unique une demande de route) est d'abord envoyé aux plus proches voisins qui vont ensuite propager le message, jusqu'à atteindre le nœud destination (ou un nœud connaissant un chemin vers celui-ci). Chaque nœud

intermédiaire enregistre dans sa table de routage l'adresse du nœud qui lui a transmis le RREQ, établissant ainsi le chemin de retour (Reverse Path). Si un nœud reçoit plusieurs copies d'un même RREQ, seule la première est conservée. Une entrée de la table de routage contient essentiellement l'adresse de la destination, l'adresse du nœud suivant, la distance en nombre de sauts (le nombre de nœuds nécessaires pour atteindre la destination), le numéro de séquence destination, le temps d'expiration de chaque entrée dans la table **[15]**. AODV utilise le numéro de séquence similaire à celui de DSDV pour éviter les boucles et être sûr d'utiliser les routes les plus récentes (la nouveauté de route). Une fois que le message atteint le nœud destination, l'activation de la route se fait par l'envoi d'une réponse de route RREP (Route REPly) vers la source qui contient un numéro de séquence plus élevé; Notons qu'un nœud intermédiaire peut aussi générer un RREP si la requête l'autorise à le faire (bit destination_only de la RREQ mis à 0) et qu'il dispose déjà dans sa table de routage d'un chemin valide vers la destination. Lors de la propagation de la réponse de route, chaque nœud intermédiaire stocke une route vers la destination. Ainsi, la source peut commencer l'envoi de données dès la réception de la réponse de route.

Dans la figure 2.8: lorsque le nœud 1 désire envoyer des données au nœud 5 et qu'aucune route n'est disponible, la source 1 diffuse en broadcast un message de demande de route RREQ (voir figure 2.8a). Le nœud 1 enregistre l'identifiant de paquet RREQ dans son historique (buffer) et l'associe à un timer qui décomptera sa durée de vie au delà de laquelle cette entrée sera effacée. Quand un nœud intermédiaire (cas des nœuds 2 et 4 dans la figure 2.8b) qui n'a pas de chemin valide vers la destination reçoit le message RREQ, il ajoute ou met à jour le voisin duquel le paquet a été reçu. Il vérifie ensuite qu'il ne l'a pas déjà traité en consultant son historique des messages traités. Si le nœud s'aperçoit que la RREQ est déjà traitée, il l'abandonne et ne la rediffuse pas. Sinon, il met à jour sa table de routage à l'aide des informations contenues dans la requête afin de pouvoir reconstruire ultérieurement le chemin inverse vers la source. Il incrémente ensuite le nombre de sauts dans la demande de route et la rediffuse.

À la réception d'un paquet RREQ (figure 2.8c), la destination 5 ajoute ou met à jour dans sa table de routage un chemin vers le nœud voisin duquel il a reçu le paquet (nœud 4) ainsi qu'un chemin vers la source 1. La destination 5 génère ensuite une réponse de route RREP qu'elle envoie en unicast vers le prochain saut en direction de la source (voir figure 2.8c). Les nœuds intermédiaires qui reçoivent la RREP (cas du nœud 4 dans la figure 2.8d) vont mettre à jour le chemin qui mène à la destination dans leurs tables de routage et retransmettre en

unicast le message (après avoir incrémenté le nombre de sauts) vers le nœud suivant en direction de la source sachant que cette information a été obtenue lors du passage de la RREQ.

Lorsque la réponse de route atteint la source (nœud 1 dans la figure 2.8e), un chemin bidirectionnel est établi entre la source et la destination et la transmission de paquets de données peut débuter.

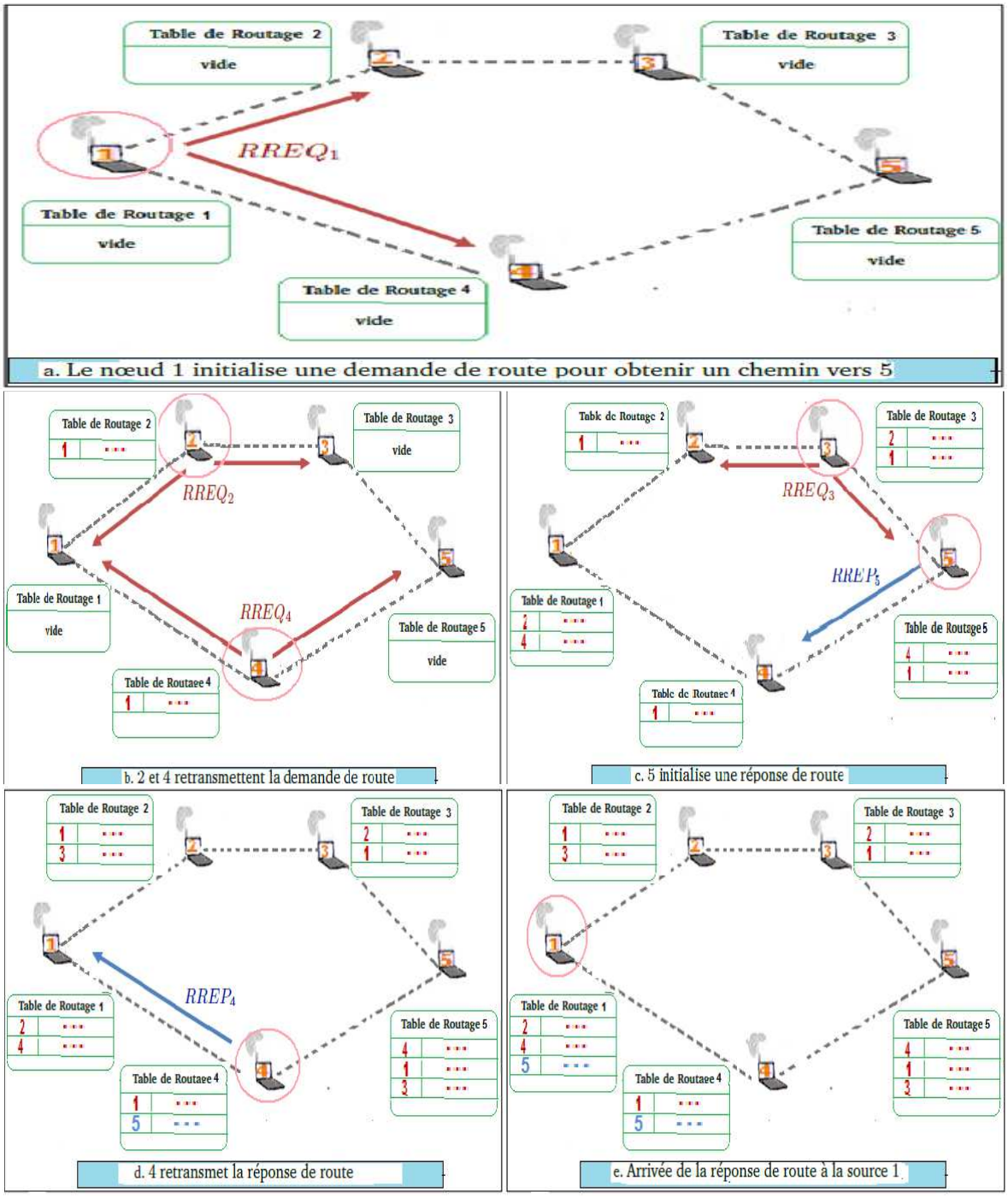

Figure 2.8. Découverte de route dans AODV.

b) La maintenance de route

De même que pour DSR, une maintenance de route est effectuée, notamment pour détecter la rupture de liens. La rupture **[33]** d'un lien peut être détectée de plusieurs façons différentes: accusés de réception de la couche MAC; accusés de réception explicites dans le protocole ou une écoute de la retransmission par le nœud suivant du paquet retransmis.

Dans le protocole AODV on peut remarquer un mécanisme simple de la maintenance de routes s'appuie sur l'échange périodique de paquets Hello, ce genre d'échange de messages permet aux nœuds voisins de signaler leur présence. En plus ces messages permettent entre autre de détecter des cassures de route : Si au bout d'un certain temps, un nœud ne reçoit plus de paquet Hello d'un voisin, le lien en question est considéré comme défaillant. Alors, un paquet d'erreur de route est diffusé vers les voisins actifs et relayé jusqu'à la source qui pourra initier une nouvelle découverte de routes. Si, dans sa table de routage, un nœud a un chemin passant par ce lien, il efface la route et recommence une recherche de chemin, s'il en a besoin.

2.5.3. Routage hybride

Afin de tirer avantages des deux protocoles précédents tout en réduisant leurs inconvénients, une nouvelle approche dite «hybrides » est aussi envisagée. Les protocoles hybrides vont utiliser à la fois des techniques proactives et des techniques réactives pour acheminer l'information. Ce type de protocoles découpe généralement le réseau en zone. Pour accélérer le processus de routage intra-zone, Ils adoptent une méthode proactive pour établir les chemins à l'avance dans un voisinage ne dépassant pas quelques sauts (2 ou 3 sauts) et utilisent une méthode réactive au delà de cette limite **[25]**. Un nœud appartenant à une zone peut décider directement à la réception d'un message si la destination fait partie de la même zone ou non, auquel cas il devra rediriger le message vers une autre zone. Parmi les protocoles de cette catégorie on va présenter dans cette section le protocole ZRP (Zone Routing Protocol).

2.5.3.1. Le protocole ZRP (Zone Routing Protocol)

ZRP **[34]** (Zone Routing Protocol) définit pour chaque nœud une zone connue sous le nom "zones de routage" (routing zone). Chaque zone de routage pour un nœud source, est définie par son "rayon de zone" qui correspond au nombre de sauts maximum qu'il peut y avoir entre un nœud destinataire et le nœud source. les paquets sont routés au sein de la zone de routage

ou bien hors de cette zone, en utilisant à chaque fois certain mode de routage. Alors Selon le protocole de routage ou le mode du travail utilisé dans chaque zone de routage, on peut distinguer **[28]** : **une zone proactive** (ou **intra-zone**) correspondant au N-voisinage au sein duquel est appliqué un modèle proactif et **une zone réactive** (ou **inter-zone**) correspondant au reste du réseau (c'est-à-dire, excluant le N-voisinage), au sein de laquelle une approche réactive est appliquée. ZRP inclut tel que définie dans **[28]** ses trois propre protocoles essentiels IARP (IntrAzone Routing Protocol) comme protocole proactif pour maintenir les informations de routage dans une intra-zone, un protocole réactif **inter-zone** nommé IERP (IntErzone Routing Protocol) et le protocole BRP (Bordercast Routing Protocol) pour but de construire la liste des nœuds périphériques d'une zone ainsi pour propager des requêtes de recherche de routes de l'IERP dans le réseau. Ce protocole présente l'avantage de diminuer le nombre de messages de contrôle qui transitent sur le réseau comparé aux protocoles proactifs ou réactifs. De plus, il permet de diminuer le temps de latence pour trouver de nouvelles routes. Le fonctionnement de ZRP en utilisant ces trois protocoles sera illustré dans la figure 2.9 en dessous :

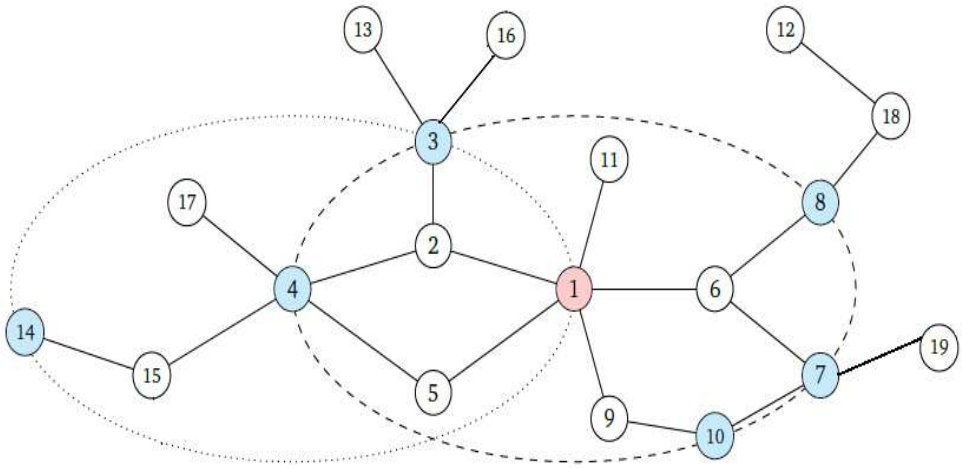

Figure 2.9. Zone de routage de rayon=2 du nœud 1 et 4.

- le protocole de routage proactif IARP fournit une vue détaillée du voisinage à k-sauts (c'est à dire définir de zone avec un rayon= k-sauts par exemple k=2 dans La figure 2.9). Cette figure présente les zones de routage pour les nœuds 1 et 4 où on voit par exemple que, pour un rayon de zone égal à deux, la zone de routage du nœud 1 est constituée par tous les nœuds qui sont autour du nœud 1 avec un maximum de deux sauts les séparant, sont donc inclus dans la zone de routage, tous les voisins du nœud 1 ainsi que tous les voisins de ces voisins. Chaque nœud maintient sa propre zone de

routage, de cette manière, un nœud peut décider immédiatement lors de la réception d'un paquet s'il a un chemin vers la destination ou non et peut ainsi répondre au nom de tous les nœuds de la zone à laquelle il appartient. Ce qui évite l'effort d'explicitement interroger le reste des nœuds de la même zone.

- Si un nœud n'a pas de chemin vers la destination, le protocole réactif IERP prend le relais pour la recherche de routes en dehors de la zone dans laquelle le nœud se trouve. Ainsi, une demande de route est créée et envoyée aux nœuds périphériques de la zone de routage. Par exemple, les nœuds 3, 4, 7, 8 et 10 sont des nœuds périphériques de la zone de routage du nœud 1 dans la figure 2.9.

Les demandes de route créées sont acheminées vers la périphérie de la zone en utilisant le protocole BRP. Ce dernier se base sur la topologie obtenue grâce à l'IARP pour la construction d'un arbre multicast (bordercast tree) donnant les différents chemins pour atteindre les nœuds périphériques d'une zone. Ces nœuds périphériques vérifient à leur tour l'existence de destination dans leurs zones et si c'est le cas, un paquet de réponse de route est retourné à la source. Dans le cas contraire, ils diffusent la demande de route à leurs propres nœuds périphériques qui, à leur tour, effectuent le même traitement. Chaque nœud retransmettant la demande de route fait attention à ne pas retransmettre la demande de route aux nœuds l'ayant déjà traité afin d'optimiser le temps de découverte de route et éviter les boucles de routage.

2.6. Conclusion

Le routage constitue une fonction principale dans le contexte des réseaux Ad hoc. Il s'agit du mécanisme par lequel les chemins sont créés pour acheminer les données à la bonne destination à travers un réseau. Nous avons vu dans ce chapitre que l'utilisation des protocoles de routage classiques, utilisés pour les réseaux filaires et ceux munis d'une infrastructure est inappropriée dans les réseaux Ad hoc puisqu'il faut prendre en considération les caractéristiques de ce type de réseaux (support de transmission, mobilité, ressources limitées, absence de centralisation, changements de la topologie du réseau etc.). Toutes ces spécificités imposent des contraintes supplémentaires aux concepteurs et aux développeurs de services informatiques dédiés aux réseaux Ad hoc et les poussent à réfléchir à de nouvelles approches de routage spécifiques aux réseaux Ad hoc. Par conséquent, de multiples recherches ont été menées et plusieurs protocoles de routage ont été développés. Ce chapitre a parcouru un certain nombre de protocoles de routage proposés dans la littérature dans le contexte des

réseaux dynamiques de type Ad hoc. On peut tout de même remarquer que la classification standard qui consiste à séparer les approches de routage en trois méthodes proactive, réactive et hybrides est de plus en plus difficile à tenir.

L'algorithme de routage consiste à assurer une stratégie qui garantit, à n'importe quel moment, la connexion entre n'importe quelle paire de nœuds appartenant au réseau. Les protocoles de routage Ad hoc tel que conçus manquent de contrôles de sécurité. La plupart font l'hypothèse d'un comportement honnête entre les entités qui collaborent. La réalité peut toutefois être très différente en présence d'entités malveillantes capables de corrompre le bon déroulement des opérations pour servir leur intérêt.

Il apparaît clairement que les réseaux sans fil Ad hoc constituent, de par leur nature, un formidable challenge pour la sécurité informatique. En effet, comme nous l'avons expliqué au premier chapitre, les spécificités de ces réseaux, qui sont principalement la transmission en milieu ouvert, les topologies dynamiques, l'absence d'autorité centrale, la nécessité de bonne coopération des nœuds, font que, les réseaux sans fil Ad hoc font appel à des solutions de sécurité originales et adaptées au contexte et aux caractéristiques de ce type de réseau.

Ainsi, nous montrons dans le chapitre qui se suit (chapitre 3), que toutes ces contraintes concourent à rendre la sécurité des réseaux sans fil Ad hoc difficile et complexe à appréhender. Ce sujet est d'autant plus critique lorsqu'on sait que le routage, considéré comme étant la clé de voûte des réseaux Ad hoc, est lui-même sujet aux vulnérabilités et attaques de déni de service, de confidentialité ou autres. Si les mécanismes de routage conçus venaient à être compromis ou détournés de la tâche pour laquelle ils ont été conçus, le réseau Ad hoc en question risquerait fort de ne plus être fonctionnel, ou du moins ne le serait plus de façon optimale.

Chapitre 3. Sécurité de routage dans les réseaux AD hoc

3.1. Introduction

La sécurité est un sujet important à traiter, surtout pour les applications de MANET dites « sensible à la sécurité » (par exemple une application du type champ de bataille). Effectivement les réseaux Ad hoc sont connus par une architecture ouverte de réseau, un milieu sans fil partagé, des contraintes rigoureuses de ressource, et une topologie de réseau fortement dynamique. Pour les réseaux Ad hoc, le principal problème ne se situe pas tant au niveau du support physique mais principalement dans le fait que tous les nœuds sont équivalents et potentiellement nécessaires au fonctionnement du réseau et surtout dans le routage des données dans le réseau, donc ces réseaux sont généralement considérés difficile à sécuriser.

Nous avons déjà signalé que le routage Ad hoc est très différent de celui des réseaux traditionnels (filaires et cellulaires). Il en est de même pour sa sécurité. La sécurité est alors devenue un souci primaire afin de fournir la communication protégée entre les nœuds mobiles dans un environnement hostile. En effet, outre les risques encourus par tout type de réseaux, les réseaux Ad hoc présentent des vulnérabilités qui leurs sont propres. Dans les réseaux Ad hoc, la sécurité concerne deux aspects, la sécurité du routage et la sécurité des données. Ces deux aspects comportent certaines vulnérabilités. Ces faiblesses rendent possible des attaques visant la confidentialité ou le déni de services attendus de ces réseaux. Nous commencerons ce chapitre par une première partie où nous énumérerons et expliquerons des faiblesses pouvant fragiliser les réseaux Ad hoc. Cette partie concernera les vulnérabilités, tel que la non fiabilité du médium d'accès, limitation des ressources ... etc.

La sécurité dépend de plusieurs paramètres (authentification, confidentialité, intégrité, non répudiation et disponibilité) qui vont être définies dans la troisième section. Nous présenterons à la quatrième section les différents schémas d'attaques possibles dont on peut distinguer deux types d'attaquant qui sont : les attaques externes et les attaques internes. Nous énumérerons par la suite des attaques pouvant exister au niveau des protocoles de routage ou de la couche réseau. Ensuite, nous nous pencherons dans la cinquième section sur les solutions et les mécanismes de sécurité qui ont été proposés dans la littérature. Beaucoup de travail de recherche a été investi pour tenter de répondre à ces lacunes sécuritaires. Ces solutions peuvent être classées en deux catégories : Des solutions à base de cryptographie (chiffrement, signature, etc.) et des solutions basées sur des systèmes de détection d'intrusion

ou des mécanismes de renforcement de coopération (solutions de gestion de réputation et de confiance). La plupart des solutions de sécurité actuelles sont basées sur des primitives cryptographiques Cependant, ces primitives sont souvent utilisées comme un moyen de prévention (par exemple, en limitant les accès des utilisateurs).Toutefois, quand l'attaquant est à l'intérieur du réseau et corrompt des nœuds légitimes afin qu'ils se comportent de manière malfaisante ou quand la cryptographie est considérée trop coûteuse, d'autres approches sont nécessaires. Le deuxième type de solutions, est un candidat intéressant dans ce contexte. Nous présenterons ainsi certains travaux proposés dans le cadre de la sécurité des protocoles de routage dans les réseaux Ad hoc basés sur la cryptographie, et d'autres travaux basés sur les systèmes de réputation. Enfin, notre conclusion est présentée dans la section six.

3.2. Vulnérabilité des réseaux Ad hoc

Les mécanismes de sécurité conçus pour les réseaux traditionnels (filaires et cellulaires) ne sont pas adaptés au réseau Ad hoc. Ses caractéristiques uniques discutées dans les sections précédentes lancent certain nombre de défis non triviaux à la conception de sa sécurité. Les nouveaux besoins de la sécurité du routage Ad hoc sont présentés dans **[35]**, **[36]**:

Nœuds compromis : les nœuds dans un MANET sont plus faciles à compromettre que ceux dans les réseaux traditionnels, parce qu'ils sont de natures mobile et sans fil, donc sont plus faciles à déplacer et à attaquer. De plus, parce qu'ils peuvent éventuellement entrer et/ ou sortir du réseau de temps à autre, et que les réseaux Ad hoc peuvent être divisés et/ ou fusionnés, les attaquants auront plus de chances d'attaquer des nœuds sans être aperçus.

Faible capacité, **ou nœuds hétérogènes** : la capacité souvent limité des nœuds et l'utilisation des batteries pour l'alimentation des équipements sont aussi des faiblesses des réseaux Ad hoc.les nœuds Ad hoc peuvent ainsi avoir une durée de vie limitée.

Manque de coopération : il faut assurer la coopération entre les nœuds parce que dans un réseau Ad hoc, les nœuds ont tendance d'être égoïstes à cause du manque de ressources. Malheureusement, il est difficile de détecter des nœuds égoïstes, ainsi quand de tels nœuds sont nombreux dans le réseau, la disponibilité du service de routage est atteinte.

Manque d'organisation : le manque d'organisation influence aussi la sécurité des MANET. Parce qu'un nœud n'a pas forcement de connaissance sur les autres lors de la montée du réseau, la confiance apriori peut ne pas exister. De plus, parce qu'il n y a pas de serveur central, la distribution et la gestion de clés peuvent être difficile à réaliser. D'autre part à

cause de la nature dynamique du réseau, il n'est pas facile de gérer l'adhésion des membres du réseau. Tous ces problèmes génèrent de sérieuses difficultés pour la sécurité du routage Ad hoc.

Mobilité : la mobilité des nœuds rend la topologie des MANETs instable. Il n'est donc pas facile pour un nœud de connaitre correctement son voisinage et la topologie du réseau. Les attaquants peuvent ainsi forger et diffuser des fausses informations de topologie pour réaliser leurs attaques. Par ce moyen un protocole de routage Ad hoc non sécurisé peut facilement être attaqué. De plus la mobilité des attaquants peut aussi les rendre plus difficile à détecter ou localiser.

Interface sans fil (radio) : A cause de la nature de radio en transmission, chaque paquet émit dans le réseau, que ce soit en unicast ou en diffusion, pourrait être reçus par tout voisin de son émetteur. De plus le problème des nœuds cachés (où des émetteurs qui ne peuvent pas entendre l'un à l'autre envoient à un même récepteur en même temps) peut causer des collisions. En outre le problème de nœuds exposés (où les nœuds dans la porté d'un émetteur d'une session en cours sont interdits d'émettre) peut gaspiller la bande passante du réseau. D'autres problèmes existent aussi dans les réseaux Ad hoc à cause d'interface sans fil tels que les pertes de paquets, l'atténuation de signal, ...etc.

3.3. Conditions de sécurité du routage dans les réseaux Ad hoc

Le service de sécurité dans un réseau mobile Ad hoc n'est pas différent de ceux des autres réseaux. Le but est de protéger l'information et les ressources des attaques et des mauvais comportements. Pour assurer la sécurisation d'un système d'information, Les services de sécurité sont basés sur quatre concepts fondamentaux **[37]** : l'authentification des utilisateurs, la confidentialité, l'intégrité des données et du trafic du réseau, et la non répudiation des utilisateurs. En ajoutant qu'il faille aussi assurer la disponibilité et la fiabilité du système.

Puisque nous nous intéressons à la sécurité des protocoles de routage, n'importe quel algorithme de routage doive intégrer dans son système un mécanisme de sécurité qui dépendra de ces facteurs, nous proposons donc de les définir dans ce contexte :

L'authentification : Cette propriété est utilisée pour fournir des services de contrôle d'accès dans le réseau Ad hoc. Avec l'authentification, au cours d'une communication dans le réseau, le destinataire sera sûr que le message provient de la source prétendue. Un nœud non autorisé

n’a pas la permission d’accès à l’information de routage ainsi il n’a pas le droit de participer au protocole de routage Ad hoc. Si l'authentification est mal gérée, un attaquant peut s'attacher au réseau et injecter des messages erronés.

La confidentialité : Une fois les entités authentifiées, la confidentialité reste un point important, elle assure que l'information (notamment les informations échangées et traitées dans les messages de routage) ne peut pas être interprétée par des tiers non autorisés au cours d’une communication dans le réseau. En raison de la portée limitée de chaque nœud, les communications entre deux nœuds sont habituellement établies à l’aide d’un certain nombre de nœuds intermédiaires. Malheureusement, certains de ces nœuds intermédiaires peuvent être malveillants, ce qui représente une menace pour la confidentialité des données échangées.

L’intégrité : assurer que la modification des données transmises sera détectée et que le message n'est jamais corrompu. Cela permet à chaque nœud d’avoir des informations correctes de routage, ceci préserve par conséquent l’intégrité de la table de routage construite à partir de ces messages. L’intégrité est souvent combiné avec l'authentification de données puisque l'intégrité des données seule ne peut pas aider des récepteurs à décider si la donnée reçue est forgée ou non **[38]**.

La disponibilité : assure que des services offerts par le nœud seront à la disposition de ses utilisateurs quand ils sont requis, c’est-à-dire la survie des services de réseau même en présence d’attaques tel que des attaques de déni de service **[19]**. Pour cela le protocole de routage doit surmonter toute tentative d’attaque de type dénis de service.

Fiabilité : vise à avoir un réseau robuste, capable de gérer des problèmes. Les réseaux Ad hoc sont souvent utilisés comme solution dans des situations de secours lorsque l’utilisation d’une infrastructure fixe est impossible. Le routage doit être fiable et des procédures de secours peuvent être exigées. Une attaque contre un réseau vise essentiellement à compromettre la confidentialité et l'intégrité des informations en transit, ou de manière plus générale, à perturber son bon fonctionnement.

Non répudiation : ce principe permet de s’assurer qu’un nœud ne peut pas refuser un message dont il est la source ; ce principe est réalisé en appliquant une méthode basé sur la signature électronique.

3.4. Attaques contre le réseau Ad hoc (MANET)

Comme toutes les technologies sans fil, dans un réseau Ad hoc, l'ensemble du trafic passe dans l'air, ceci constitue une vulnérabilité qui peut aisément être exploité par un attaquant, et l'écoute s'avère donc très simple. Une attaque est en fait toute circonstance ou évènement susceptible de nuire à un système grâce à un accès non autorisé, afin d'atteindre un objectif (interrompre, perturber, absorber, ou attirer le trafic et même provoquer un déni de service). Les attaques dans un réseau Ad hoc peuvent paraître comme étant des attaques **passives** tentant d'accéder à des informations échangées sur le réseau, sans altérer les opérations du réseau ou bien des attaques **actives** tentant d'altérer les opérations et les ressources du système ou d'affecter leurs activités.

Les protocoles de routage Ad hoc tel que conçus, manquent de contrôles de sécurité, ce qui augmente le risque d'attaques , un nœud malveillant peut donc détourner le fonctionnement normal du protocole de routage en émettant de fausses informations dans les messages de contrôle échangés entre les nœuds comme Il peut aussi s'attaquer aux paquets de données en les détruisant, en les modifiant ou en les réémettant plus que nécessaire. Pour qu'un protocole de routage pour les réseaux Ad hoc soit efficace, il doit donc être conçu pour contrecarrer les deux types d'attaques actif et passif.

3.4.1. Attaque passive

Les attaques passives constituent une menace non-ignorable à la sécurité et à l'intimité du réseau, le nœud malicieux pourra jouer sur la localisation et s'approcher des nœuds qu'il souhaite surveiller pour en capturer le trafic sans aucune intervention **[39]**. L'action de l'attaquant peut se résumer à écouter ou surveiller les transmissions. Le but est d'obtenir les informations qui transitent soit directement soit après une analyse, Si l'adversaire a réussi à interpréter les données capturées, la propriété de la confidentialité est violée **[40]**. Ce type de comportement est très difficile à détecter puisque le nœud malhonnête n'altère pas les messages échangés et ne participe pas en envoyant des messages supplémentaires. L'écoute passive est souvent une des premières actions de l'attaquant pour essayer d'obtenir un maximum d'information sur sa cible ou bien de connaitre les nœuds importants dans le réseau, pour la faire, le nœud malicieux va devoir intervenir sur protocole de routage pour s'assurer que le trafic qu'il souhaite surveiller passe bien par lui, ensuite ces informations

servant de support à la réalisation d'attaques plus complexes. Par exemple une attaque par déni de service ciblant les nœuds importants peut faire tomber le réseau (mettre en disfonctionnement).

3.4.2. Attaque active

Les attaques actives peuvent être orchestrées par des nœuds externes ou internes en tenant compte du positionnement du nœud malhonnête par rapport au réseau **[40].** Les attaquants externes sont des nœuds qui ne font pas partie du réseau. Cependant les attaquants internes sont des nœuds faisant légitimement partie du réseau (ces nœuds ont les autorisations nécessaires pour appartenir au réseau et les autres nœuds leur font a priori confiance). Les attaques internes sont plus difficiles à détecter et à éviter que les attaques externes. Dans le cas des attaques externes, la mise en place de mécanismes cryptographiques peut résoudre le problème : seuls les nœuds ayant les autorisations nécessaires pourront accéder au réseau ou déchiffrer le contenu. Par contre les attaques internes requièrent de mettre en place des mécanismes de détection des nœuds attaquants et des mécanismes pour contrer leurs agissements.

Il est à noter que certaines attaques peuvent être de type individuelles ou par collusion. Les attaques individuelles sont relativement simples, menées par un seul nœud attaquant. En revanche, les attaques par collusion, issues de plusieurs nœuds repartis à différents endroits dans le réseau qui mutualisent leurs informations et leurs ressources, en exploitant les connexions qu'ils ont entre eux, sont généralement plus évoluées et plus pernicieuses.

Quelque soit sa position (interne ou externe), lors de ses attaques, le nœud malhonnête utilise une ou plusieurs techniques (rejeu, modification, suppression, fabrication) pour perturber le bon fonctionnement du protocole. La combinaison de ces techniques peut aboutir à une attaque plus élaborée et par conséquent elle peut violer une propriété de sécurité ou plus. Les nœuds malhonnêtes peuvent s'attaquer à la disponibilité des nœuds. C'est le cas de l'attaque par consommation des ressources des nœuds, comme le cas pour des attaques de DoS (déni de service : Denial of Services), ou attaques de rupture de cheminement visent à perturber l'opération normale des protocoles de cheminement en laissant tomber défavorablement et/ou en modifiant des paquets de cheminement et en diffusant frauduleux l'information incorrecte de cheminement **[41]**, **[39]**. L'intégrité de la topologie peut être compromise par fausse de table de routage à partir du moment où un attaquant génère des

messages de contrôle dont le contenu n'est pas conforme au regard de la logique du protocole, ou bien s'il ne participe pas correctement à la retransmission de ces messages.

Nous présentons dans ce qui suit à des fins d'illustration une liste non exhaustive des attaques sur les protocoles de routage Ad hoc présentées dans la littérature :

3.4.2.1. Déni de service (DoS : Denial of Services)

Les réseaux Ad hoc se caractérisent par des ressources limitées en termes d'énergie et de bande passante. Les dénis de services, apparaissent comme les attaques les plus faciles à réaliser par un attaquant. C'est une technique consiste à consommer les ressources en sollicitant de manière continue le nœud cible, en fabriquant des messages inutiles (sans signification particulière) à destination de la cible ou en modifiant des paquets pour que les messages passent par la cible, ce qui provoque des traitements supplémentaires. Ceci dans le but d'augmenter la charge sur le réseau ainsi que d'épuiser les ressources des nœuds **[22]**.

Une attaque de dénis de services se dégage plus particulièrement dans le cas de réseau Ad hoc **[36]** :

- ✓ Brouillage du canal radio pour empêcher toute communication.
- ✓ Tentative de débordement des tables de routages des nœuds servant de relai : Ceci passe par la création de demandes de routes ou de messages de mise à jour pour des nœuds non existants jusqu'à débordement de la table de routage de la cible ce qui empêchera la formation de routes réelles.
- ✓ Dispersion et suppression du trafic en jouant sur les mécanismes de routage.
- ✓ …

3.4.2.2. Le rejeu

Les messages de contrôle échangés entre les nœuds décrivent un état de la topologie du réseau à un instant donné. Une attaque qui exploite ces informations est le rejeu. Une particularité de cette attaque est qu'elle est effective même si les messages de contrôle sont protégés par une empreinte ou une signature numérique **[22]**. Elle consiste en la réémission en un point du réseau de messages de contrôle caducs (le nœud malhonnête enregistre une séquence de trafic qu'il réinjecte ensuite dans le réseau). La conséquence est que des nœuds sont amenés à réaliser des mises à jour sur une base d'informations qui n'a plus lieu d'exister, entrainant alors des incohérences dans les chemins construits.

3.4.2.3. Attaque de trou de ver (Wormhole attack)

L'attaque de trou de ver se base sur le rejeu de messages (voir figure 3.1). Elle nécessite au moins deux adversaires géographiquement séparés et la mise en place d'un tunnel de communication privé entre eux. Un attaquant reçoit les paquets d'un nœud légitime et il les envoie à travers un tunnel à l'autre attaquant de collaboration qui rediffuse les paquets à ses voisins. Le but du tunnel est de faire croire aux autres nœuds du réseau que les deux extrémités du tunnel sont voisines alors qu'en réalité ils sont distants de plusieurs sauts. Ce genre d'attaque est une menace très dangereuse contre des protocoles de routage parce qu'il force tous les itinéraires à passer par le tunnel de trou de ver **[43]**.

Le tunnel dans cette attaque créé peut être une liaison physique directe ou une liaison virtuelle :

- ✓ un nœud malveillant encapsule un paquet reçu d'un de ses voisins et il l'envoie à un autre nœud malveillant situé dans un voisinage différent, pour former un lien de voisinage virtuel.
- ✓ les nœuds malveillants créent un tunnel de trou de ver en utilisant un canal externe à haut débit. Ce canal peut être un lien de câble ou un lien sans fil à haute fréquence différente.

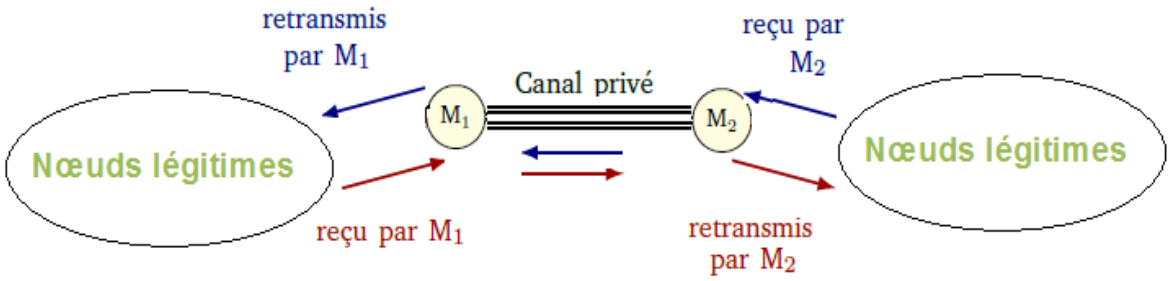

Figure 3.1. Attaque de trou de ver.

3.4.2.4. Attaques par suppression de paquets

C'est une attaque selon laquelle un intrus supprime les messages de contrôle qu'il reçoit au lieu de les retransmettre. Elle entraine non seulement une réduction de la connectivité globale et du nombre de chemins de communication disponibles, mais aussi un raccourcissement de la durée de vie du réseau puisque le trafic sera moins bien répartis entre les nœuds.

On peut trouver deux types de ces attaques:

- **Trou noir (Black holes)** : Dans ce cas de figure, un nœud malhonnête tente d'exploiter les failles des protocoles de routage afin de se faire élire comme faisant partie du plus court chemin vers le nœud dont il veut intercepter les paquets. Le nœud malveillant par la suite capte et absorbe les paquets transmis (contrôle et donnée), puis il les supprime au lieu de les retransmettre pour exécuter un DoS par exemple **[40]**. (La figure 3.2 illustre ce type d'attaque).
- **Trou gris (Gray holes)** : C'est un cas particulier du trou noir dans lequel l'attaquant supprime les paquets de données et transmet ceux de contrôle **[42]**. Ce type d'attaque est ainsi plus difficile à détecter que l'attaque du trou noir.

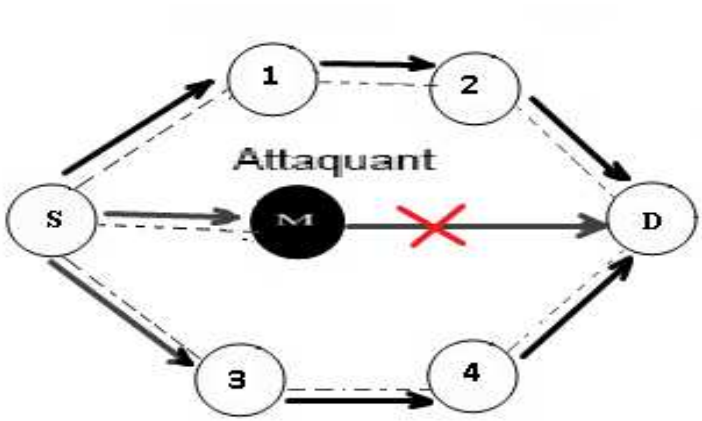

Figure 3.2. L'attaque de trou noire dans MANET.

Toutefois, il est à noter que cette attaque peut être également confondue avec le fait qu'un nœud est soit surchargé, soit incapable (nœud à faible capacité) de jouer le rôle d'un routeur, ce qui peut compliquer la détection de ce genre d'attaques.

3.4.2.5. Attaques par modification des informations de routage

C'est la manière la plus simple pour qu'un nœud malveillant touche aux opérations d'un réseau Ad hoc. En absence de contrôle d'intégrité sur les messages transmis, un attaquant met à jour une valeur de métrique pour une route ou certains champs des messages de contrôle qu'il reçoit et les retransmet, sans suivre les recommandations du protocole de routage, un nœud malicieux peut rediriger le trafic vers lui ou causer un déni de service. Parmi ces champs : le numéro de séquence, le nombre de sauts, les identités des nœuds (adresses IP), le descriptif du chemin en construction.

3.4.2.6. Attaques par usurpation d'identité (Spoofing)

Plus généralement connues comme 'spoofing', puisque le nœud malveillant cache son adresse IP et/ou MAC et utilise celle d'un autre nœud légitime du réseau. L'intrus ensuite peut lancer ses attaques avec l'identité de ce nœud. Par exemple **[44]**, un attaquant peut créer des boucles de routage dans le réseau pour isoler un nœud du reste du réseau. Pour faire ceci, l'attaquant doit personnifier l'adresse IP du nœud qu'il veut isoler dans le réseau et puis annonce la nouvelle route aux autres nœuds. En faisant ceci, il peut facilement modifier la topologie de réseau comme il veut.

3.4.2.7. Attaques par fabrication de messages

La détection de ces attaques est très difficile. Elles consistent à générer des informations de routage falsifiées ensuite les injecter dans le réseau. Les paquets injectés proposent par exemple des routes plus courtes, plus fraiches, de nouvelles routes non-existantes ou même des routes à supprimer.

3.4.2.8. Rushing attack

Cette attaque peut être utilisée pour améliorer la fabrication des messages de la route en profitant que dans plusieurs protocoles de routage, certains types de messages de route ont la propriété que seul le message qui arrive le premier est accepté par un récepteur **[45]**. Dans l'attaque Rushing, l'attaquant alors exploite cette propriété en retransmet plus rapidement les messages pour bloquer les messages légitimes qui arrivent plus tard et pour que la route qui passe par lui soit retenue. Une fois le nœud malhonnête sur la route, il peut absorber totalement ou sélectivement le trafic. En effet, cette attaque s'appuie sur le fonctionnement des protocoles de routage réactifs et plus précisément sur la diffusion des paquets de demande de route. Cela est possible en ne respectant pas, par exemple, les délais de transmission des paquets de demande de route tels qu'ils ont été spécifiés par le protocole de routage ou bien en ne respectant pas les délais d'accès aux médias de communication.

3.4.2.9. Sybil attack

C'est une variante de l'attaque Spoofing où le nœud malhonnête revêt plusieurs identités (possède illégitimement plusieurs identités) et se comporte comme s'il était un ensemble de nœuds **[46]**. Par exemple, pour attaquer un protocole de routage, l'attaque Sybille peut donner l'illusion à un nœud de posséder plusieurs chemins vers une destination alors que tous ces chemins traversent la même entité physique.

3.5. Solutions et mécanismes de sécurité

La littérature est riche de plusieurs mécanismes et de propositions pour sécuriser les protocoles de routage Ad hoc. Pour défendre contre les attaques discutées en section (3.4), les protocoles proposés se concentrent pour la plupart sur l'authentification des nœuds source et destination afin de garantir qu'aucun attaquant ne peut usurper l'identité de l'un des deux nœuds communicatifs. Cette défense est adaptée surtout pour défendre contre des menaces externes. Cependant, elle reste inefficace contre des attaques à partir des nœuds compromis. Cet aspect laisse en tout cas présager l'avènement de nouveaux modèles développés autour des concepts de communautés de plus en plus proches des modèles sociaux comme la réputation, le crédit, ou la recommandation.

Nous classons ces solutions en deux catégories **[43], [37]**:

- Première ligne de défense ou mécanismes de prévention dans le sens où des mécanismes sont établis à l'avance pour assurer la sécurité en renforçant la résistance du système aux attaques grâce notamment aux solutions à base de cryptographie : encryptage, authentification, signatures digitales, contrôle d'accès …
- Deuxième ligne de défense ou mécanismes réactifs qui réagissent (adaptation/prise de décision immédiate) selon le comportement du voisinage et qui est lui même divisé en : systèmes de détection d'intrusion, mécanismes de renforcement de coopération (solutions de gestion de réputation et de confiance).

3.5.1. Solutions basées sur la cryptographie

Les solutions basées sur la cryptographie sont souvent utilisées contre les attaquants externes. Ces solutions font la distinction entre les nœuds qui ont les autorisations nécessaires de participer au réseau, qui sont supposés se comporter correctement et les nœuds qui n'y sont pas autorisés et qui sont considérés a priori comme étant des attaquants. La plupart de ces solutions se basent sur des mécanismes classiques de chiffrement symétrique ou à clé public ou utilisent des systèmes de suite de haché, de certificat et de signature numérique pour assurer l'authentification des nœuds, la confidentialité, l'intégrité et la non-répudiation des messages. Cependant, l'utilisation de ces mécanismes suppose l'existence d'une autorité centralisée (pour la certification ou la distribution de clés), ce qui n'est pas toujours évident dans un réseau Ad hoc. De plus, ces mécanismes n'empêchent pas certains nœuds

malhonnêtes de servir leurs intérêts par exemple en fournissant délibérément de fausses informations aux autres nœuds. Il existe néanmoins plusieurs protocoles de routage sécurisés utilisant les mécanismes cryptographiques comme ARAN, SAODV, ARIADNE, SEAD, SRP,...Nous présentons dans ce qui suit quelques protocoles de cette catégorie.

3.5.1.1. ARAN (Authenticated Routing Ad hoc Network)

ARAN (Authenticated Routing for Ad hoc Networks) est conçu sur AODV, c'est un protocole réactif basé sur la demande de route **[38]**. Avec ce protocole, les auteurs ne se contentent pas seulement de l'authentification des nœuds de bout en bout, ils proposent un service de non-répudiation en utilisant des certificats préétablis distribués par un serveur de confiance. Le rôle de serveur est de gérer les certificats (il délivre à chaque nœud X entrant dans le réseau un certificat contenant entre autre l'identifiant de X et une clé publique que X a choisi, dont la clé publique est connue de tous les participants). Le certificat d'un nœud est utilisé pour s'authentifier auprès d'autres nœuds voisins pendant le procédé de construction de route.

Le principe d'ARAN est sécuriser le mécanisme de découverte de routes de nœuds en nœud. Ainsi lorsqu'un nœud source désire connaître le chemin vers une destination, Il initie sa découverte de route en diffusant un paquet de découverte de route (RDP : Route Discover Packet). Ce RDP contient l'identification de destination, un certificat de la source, une valeur aléatoire, et un horodateur (timestamp) **[41]**. Une valeur aléatoire et un horodateur (timestamp) du paquet RDP assurent ensemble la fraîcheur du paquet (Ils sont pour but d'empêcher des attaques de rejeu et pour détecter le bouclage). Avant transmission d'un RDP, la source le signe en utilisant sa clé secrète (privée). Le premier voisin recevant le paquet vérifie la validité de la signature et la validité du certificat de la source avant de signer le message avec sa signature et son certificat. Par la suite chaque nœud intermédiaire vérifie la signature et le certificat du nœud duquel il a reçu le message et les remplacent par sa signature et son certificat et ainsi de suite jusqu'à ce que le message atteigne la destination. À l'arrivée, la destination s'assure de l'identité de la source puis répond en unicast, par un message de type RREP (reply packet) qui est à son tour vérifié de nœuds en nœuds en effectuant le même procédé de la découverte de route. Des paquets de route erronée sont également signés par leurs initiateurs **[41]**; une valeur aléatoire et un horodateur sont aussi bien employés dans chaque paquet d'erreur d'itinéraire pour assurer la fraîcheur du paquet.

Puisqu'ARAN est basé sur la cryptographie de clé publique, il est robuste contre presque toutes les attaques connues. Cependant l'inconvénient de cette méthode est qu'elle utilise l'authentification saut par saut en vérifiant à chaque fois le certificat ce qui augmente considérablement le calcul au niveau de chaque nœud ainsi que la taille des messages, cela peut se révéler extrêmement coûteux et consomme plus de bande passante. Par conséquent, ARAN est vulnérable aux attaques de DOS où les attaquants inondent le réseau avec les paquets d'acheminement forgés pour lesquels la vérification de signature est nécessaire.

3.5.1.2. SAODV

L'extension SAODV proposée par Zapata et al. **[47]** combine l'utilisation de chaines de hachage et de signatures pour garantir l'authentification de la source et l'intégrité des messages. Conceptuellement, les messages de routage de SAODV (Route REQuest : RREQ et Route REPly : RREP) ont une partie constante (non mutable) et une autre non constante (mutable). La fonctionnalité de base de SAODV se situe en sécurisant le protocole ADOV par l'authentification des données statiques du message de routage en utilisant les signatures numériques afin de contrer les attaques de type "usurpation d'identité". Elle fournit également une authentification et une vérification bout à bout de nœud-à-nœud de ces messages et seule la source signe les messages et ce uniquement sur les champs qui ne changent pas afin de limiter le coût en CPU et la taille des messages, contrairement à ARAN dans lequel les messages sont signés à chaque retransmission. La partie non constante la plus sensible reste le compteur de sauts dans les requêtes et celui-ci ne peut pas être simplement vérifié par une signature. Par conséquent, les auteurs proposent en plus l'utilisation de deux chaînes de hachage pour vérifier que le compteur de sauts n'a pas été décrémenté abusivement. Le processus souligné est relativement simple : Le nœud de source signe digitalement le paquet de demande d'itinéraire (RREQ) et l'envoie à ses voisins. Quand un nœud intermédiaire reçoit un message de RREQ, il vérifie d'abord la signature avant de créer ou mettre à jour un itinéraire renversé à son prédécesseur. Il sauvegarde alors ou met à jour l'itinéraire seulement si la signature est vérifiée. Une procédure similaire est suivie pour le paquet de réponse d'itinéraire (RREP) **[38]**.

Comme pour ARAN, des services d'authentification, l'intégrité et la non-répudiation de bout en bout, entre le nœud source et destination, sont ainsi obtenues. Cependant, SAODV présente l'inconvénient que les nœuds doivent utiliser un serveur en ligne afin de vérifier les signatures numériques et cette dernière technique de protection par utilisation des chaines de

hachage pour contrer les manipulations illégales sur le compteur de sauts n'est toutefois pas totale **[22]**. La valeur de compteur du nombre de sauts peut être rendue par un nœud malveillant supérieur ou inférieur à sa valeur réelle. Donc, le nœud malveillant peut faire apparaitre les routes plus courtes ou plus longues qu'elle n'est en réalité. D'autre part, dans l'éventualité où l'attaque de trou noir est une attaque très grave pour AODV, une attaque, encore très grave de type trou de ver où il y aurait plusieurs attaquants complices, peut toujours être lancée. SAODV est adéquat pour résoudre le problème de la première attaque mais il ne détecte pas les attaques de trou de ver **[40]**.

3.5.1.3. ARIADNE

Dans le but de proposer un mécanisme adapté à la nature spontanée des réseaux Ad hoc et aux capacités de calcul parfois restreintes des nœuds qui le composent, une extension à DSR appelée ARIADNE est proposée pour authentifier les messages de routage **[48]**, tout en garantissant un moyen de sécurisation à faible coût. Cette solution ainsi assure une authentification point-à-point des messages de routage en utilisant les fonctions de hachage à clé secrète (HMAC Hash-based Message Authentication Code). Cependant, pour assurer une authentification sécurisée, ARIADNE se base sur TESLA (Time Efficient Stream Loss-tolerent Authentication) **[48]**, **[40]**, qui est un arrangement d'authentification efficace d'émission (permet à une destination d'authentifier la source d'un message diffusé sur le réseau) à condition que les nœuds ont une synchronisation approximative de leurs horloges. ARIADNE a recours à l'utilisation de chaines de hachage à sens unique pour garantir l'intégrité de la liste des nœuds incluse dans la demande **[22]**. Chaque nœud a une clé secrète qui lui permet de calculer une chaine de hachés qui est utilisée par la suite de la manière suivante : lorsqu'il transmet un message de demande de route (RREQ : Route REQuest), le nœud lui ajoute un HMAC calculé sur l'ensemble du message avec le dernier haché encore non-utilisé de la chaine. Si un message de réponse de route (RREP : Route REPly) passe par le nœud, celui-ci révèle la pré-image de la valeur qu'il avait utilisée dans le message RREQ. Lorsque tous les nœuds sur le chemin réalisent cette opération, le chemin est authentifié.

Grâce à ce mécanisme, ARIADNE limite les attaques par modification des données variables incluses dans les messages de contrôle. Ce mécanisme permet à un nœud destinataire d'authentifier chaque nœud inclus dans la demande avant d'envoyer un message de réponse. En revanche, TELSA occasionne une augmentation du délai d'authentification, ce qui vient au détriment de la réactivité du protocole. Le mécanisme de signalisation des

ruptures offre cependant la possibilité pour les nœuds malveillants d'envoyer de fausses notifications de rupture, afin de rompre effectivement le lien en aval **[33]**. Ceux-ci peuvent aussi tâcher de se placer de façon à prendre part à un maximum de chemins et ainsi provoquer un déni de service. En outre, ARIADNE affiche des faiblesses face aux attaques par collusion de nœuds internes.

3.5.2. Système de détection d'intrusion (IDS)

Puisque les systèmes de sécurité basés sur la cryptographie sont parfois couteux et qu'ils ne permettent pas d'empêcher toutes les catégories d'attaques, d'autres travaux, souvent considérés comme complémentaires à la prévention, ont porté sur la conception de mécanismes de détection d'intrusions. Quand les mécanismes de prévention ont échoué, la détection d'intrusion est très importante pour la sécurité dans MANETs due qu'elle peut être un deuxième mur de la défense **[43]**. En effet, si une tentative d'intrusion (toute action visant à compromettre l'intégrité, la confidentialité ou la disponibilité d'une ressource) est détectée suffisamment tôt, les réponses du système peuvent permettre de limiter les conséquences d'une attaque. L'attaque d'un système peut être réalisée simplement à partir de l'enchaînement d'opérations élémentairement autorisées ; elle ne nécessite donc pas toujours de contourner les mécanismes de sécurité **[10]**. Un IDS (Intrusion Détection Systems) est un équipement permettant de surveiller l'activité d'un réseau ou d'un nœud, afin de détecter toute tentative d'intrusions et éventuellement de réagir à cette tentative. Tout d'abord, IDS ne devrait pas apporter de grandes modifications sur des protocoles de cheminement pour garder la performance et la scalabilité. En second lieu, il doit être sensible aux modèles reconnaissants d'attaque et adaptable au changement fréquent de l'environnement dans les réseaux Ad hoc **[49]**. Un IDS doit :

- traduit par une détection parfaite des attaques avec un risque minimal de faux positifs.
- être rapide en détection des intrusions avec une analyse approfondie des événements est indispensable pour mener une détection efficace en temps réel.

  Cela permet d'entreprendre instantanément les contre mesures nécessaires pour stopper l'attaque et protéger les ressources du réseau et du système de détection d'intrusions.
- résister aux attaques ainsi qu'à leurs conséquences.

Les techniques de détection d'intrusions utilisées dans les réseaux traditionnels ne peuvent être exploitées telles quelles dans les réseaux Ad hoc. En l'absence de point de concentration, la détection d'intrusions doit être distribuée sur l'ensemble des nœuds actifs à l'intérieur du réseau. De plus, dans un réseau sans fil Ad hoc chaque nœud possède une vision limitée de l'activité du réseau. Cette limite constitue une autre contrainte importante pour les algorithmes de détection des intrusions. Sans possibilité d'analyse globale des activités du réseau, la détection des intrusions est plus difficile.

3.5.3. Mécanismes de renforcement de coopération

Les réseaux Ad hoc, dans leur fonctionnement sont basés sur la coopération entre les nœuds; les nœuds doivent alors participer effectivement au réseau. On peut distinguer deux comportements qui vont nuire aux réseaux Ad hoc, l'égoïsme et la malveillance **[39]**.Un nœud deviendra égoïste dans le but de préserver ses ressources (en bande passante, en énergie, etc.). Un tel nœud a deux raisons principales pour refuser de coopérer : une telle opération induit un certain coût ; de plus, cette transmission peut introduire un délai plus ou moins important dans la transmission de ses propres paquets. Par exemple, un nœud égoïste pourra ne plus remplir son rôle de router ou se contenter de router les petits paquets (moins couteux). Un nœud malveillant ira plus loin, c'est celui qui, intentionnellement, essaie d'attaquer le système : atteinte à l'intégrité des données, à la disponibilité du service, à l'authenticité des entités (nuire le réseau par une des attaques vus dans les sections précédente).

Les mécanismes discutés précédemment ne se révèlent pas du tout adaptés pour résoudre le problème de non-participation des nœuds. C'est pourquoi certains protocoles visent plus spécifiquement l'incitation à la coopération **[50]**. Parmi ceux-ci, on distingue généralement les mécanismes qui se basent sur une réputation des nœuds élaborée au cours du temps en fonction des observations, et les systèmes de gestion de confiance.

3.5.3.1. Les systèmes de réputation et de gestion de confiance

Lorsque l'observation seule ne permet pas une mesure directe et objective de la malveillance des nœuds, il est nécessaire que chaque nœud maintienne un degré de confiance en chacun des autres nœuds qu'il a observés **[33]**. Un mécanisme de sécurité est basé sur le concept de réputation (confiance) et sert pour établir un lien entre le comportement d'un nœud et l'utilisation du réseau **[51]**. Les systèmes de réputation sont un nouveau paradigme proposé pour améliorer la sécurité dans les réseaux Ad hoc. Ce sont inspirés de nos comportements sociaux. Comme dans notre vie quotidienne quand on rencontre quelqu'un pour la première

fois on lui attribue une réputation (concernant un sujet) sur la base de notre propre expérience et celle de quelqu'un d'autres. Les systèmes de réputation sont fondés sur ce principe, et sont utilisés pour décider à qui faire confiance, et pour encourager le comportement bienveillant. Un système de réputation a pour objectif d'encourager les nœuds à agir d'une manière fiable et de décourager les nœuds indignes de confiance de participer à fournir les services protégés par le système de réputation. Il permet d'identifier au sein du réseau des nœuds non coopératif, en propageant leur réputation non-coopérative (valeur faible de confiance) à toutes les entités du réseau. Un nœud avec une faible réputation ne pourra pas se servir du réseau, il sera donc écarté du réseau.

A la différence des IDS traditionnels où les nœuds vérificateurs surveillent et analysent chacune des activités indépendamment de l'autre dans la plupart des cas, dans les systèmes de réputation chaque nœud maintient une valeur de réputation concernant le comportement global de chacun des autres nœuds qu'il a observés. Ces valeurs représentent leurs degrés de confiance et peuvent être ajustés par les différentes observations captées au cours du temps. Dans les MANET, les systèmes de réputation requièrent que chaque nœud doive en continu surveiller les activités de ses voisins.

On peut dans cette section citer un des premier travaux pour atténuer les conséquences d'un comportement malhonnête basé sur la surveillance des nœuds voisins et adaptant le routage en conséquence. Cette méthode repose sur l'emploi de deux composants distincts, un watchdog qui va surveiller les voisins et modifier la confiance que l'on a en eux selon leur comportement et un parthrater qui va s'occuper de ne router le trafic qu'à travers les nœuds dignes de confiance. Le mécanisme de surveillance du voisinage (watchdog) apparait par la suite dans la majorité des travaux de recherche de gestion de la confiance et de la réputation adaptés aux réseaux Ad hoc, dont CONFIDANT **[52]** et CORE **[53]** qui constituent un exemple de ces systèmes.

3.5.3.1.1. Mécanisme Watchdog and Pathrater

Marti et al. **[54]** proposent un système basé sur la réputation. Dans ce modèle, chaque nœud surveille son voisin pour assurer qu'il transporte les paquets des autres nœuds dont le but de contrer les comportements douteux que peuvent avoir certains nœuds du réseau. Pour cela, ils proposent deux outils : un watchdog qui identifie les nœuds non coopératifs et un Pathrater pour sélectionner les routes qui évitent ces nœuds.

Le Watchdog est le processus de contrôle exécuté par chaque nœud, pour vérifier que le nœud suivant situé sur la route achemine correctement les paquets. La figure 3.3 ci-dessous présente le mécanisme Watchdog :

S veut envoyer un paquet à D suivant un chemin direct passant par les nœuds intermédiaires A, B et C. Lorsque le nœud A transmet le paquet à B pour qu'il l'envoie à C, il ne peut pas directement communiquer avec C mais il peut écouter le trafic de B. suivant ce mécanisme il est capable de savoir si B a réellement transmis le paquet. Si le nœud B ne retransmet pas le paquet au bout d'un certains temps, le nœud A peut conclure que le nœud B est malicieux. Sa décision est rapportée au nœud S.

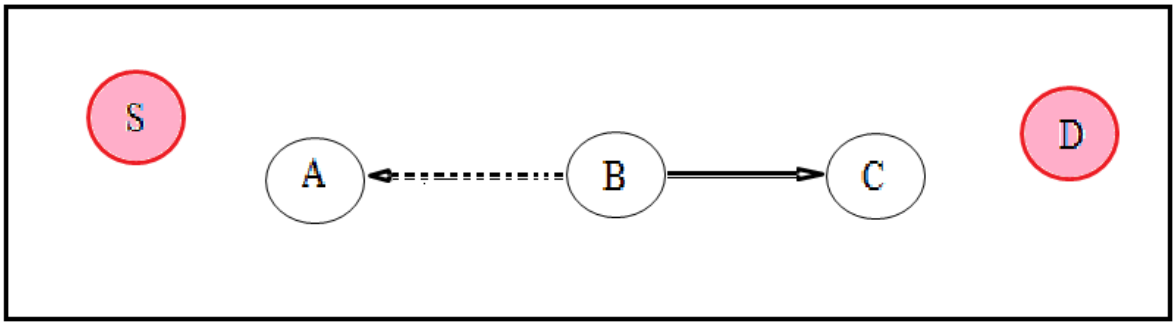

Figure 3.3. Principe de surveillance par Watchdog.

Le Pathrater exploite les informations collectées grâce au Watchdog pour éviter d'inclure les nœuds malveillants lors du processus de construction de route. Il attribue des poids ou des scores pour un certain ensemble de nœuds **[55]**. Au début, les nœuds sont assignés à un score dit neutre, ce score est réévalué suivant le nombre de paquets retransmis. On peut noter que les scores des nœuds qui ne sont pas chargés de retransmettre les paquets restent inchangés.

Cette technique permet d'augmenter les performances du réseau en utilisant les nœuds disponibles (non suspects) pour le routage et le relais des paquets. Cependant elle présente les limites suivantes **[55]** :

- Un nœud n'est pas toujours capable de capter les transmissions de ses voisins à cause des potentielles collisions ou lorsqu'un voisin utilise une puissance de signal différente (dans le cas où les liens entre les nœuds ne sont pas symétriques).
- Un attaquant qui possède une antenne unidirectionnelle, peut l'orienter de telle manière que le prochain relai ne peut pas capturer le paquet et seul l'émetteur peut le faire, et de cette manière l'attaquant reste indétectable.

- Le Watchdog n'utilise pas les outils cryptographiques, donc il est vulnérable à l'attaque Spoofing.
- Les nœuds détectés comme égoïstes ne sont pas sanctionnés.

3.5.3.1.2. CONFIDANT

Buchegger et Le Boudec **[52]** ont proposé une extension au protocole de routage DSR appelé CONFIDANT (COoperation of Nodes, Fairness In Dynamic Ad-hoc NeTworks), c'est un système de renforcement de la coopération distribué et collaboratif, CONFIDANT utilise un mécanisme similaire au mécanisme Watchdog et Pathrater. Chaque nœud dispose d'un mécanisme d'observation pour contrôler le comportement de ses voisins. Une fois qu'un comportement malicieux est détecté, le nœud malveillant est isolé et ne peut plus être sollicité pour le routage des paquets. Pour le faire, CONFIDANT applique au niveau de chaque nœud quatre éléments complémentaires interagissant entre eux : un moniteur ; pour détecter toute activité malicieuse. Il collecte des informations de première main sur le comportement des nœuds dans le réseau. En écoutant le canal radio, il vérifie autant que possible que ses voisins se comportent bien en termes de participation au protocole de routage et de retransmission des paquets. Les observations servent à classifier directement un nœud comme bienveillant ou malveillant. Si un cas suspect est détecté, le moniteur envoie une notification au système de réputation qui, à son tour, combine les informations de seconde main avec les informations de première main pour faire une mise à jour de sa table de réputation en fonction des rapports d'activités reçus sur chacun des nœuds. Si la valeur de réputation dépasse un seuil critique, une alarme est envoyée aux autres nœuds via un gestionnaire de confiance ; en effet c'est lui qui décide à quel moment un message d'alarme doit être envoyé aux autres nœuds de confiance afin de les avertir du comportement malveillant d'un nœud et c'est aussi lui qui décide si le contenu d'un message d'alarme doit être considéré ou ignoré. Ainsi un gestionnaire de chemins supprime toutes les routes contenant le nœud malicieux afin d'exclure les nœuds malveillants du réseau.

Puisque ce protocole permet l'envoi d'alarmes, le réseau peut être sujet à des attaques envoyant de fausses accusations. Ainsi, un dénie de service peut être facilement réalisé. Pour cela une version améliorée de CONFIDANT est proposée **[50]**, elle utilise une approche bayésienne afin de différencier plus efficacement les vraies alarmes de mensonges destinés à faire baisser la réputation d'un nœud.

3.5.3.1.3. CORE

CORE [53] (COllaboratif REputation mechanism) est un mécanisme collaboratif de réputation qui a été proposé par Michiardi et Molva pour contrer le comportement égoïste des nœuds. La solution consiste à offrir des moyens d'incitation pour tout nœud voulant participer aux processus collaboratifs. Les moyens d'incitation sont inspirés de la théorie des jeux. Chaque nœud a une réputation à mettre en jeu traduisant son honnêteté. Pour transmettre ou recevoir un paquet, le nœud doit avoir une réputation suffisante.

Le fonctionnement de CORE est très similaire à celui de CONFIDANT, il est basé lui aussi sur le protocole de routage DSR et repose sur des moniteurs qui analysent le trafic et qui transmettent les résultats à un système de gestion des réputations. La différence essentielle avec CONFIDANT réside dans la manière dont CORE calcule les valeurs de réputation. CORE contient une procédure de réputation sophistiquée différencie des réputations subjectives (observations), des réputations indirectes (recommandations), et des réputations fonctionnelles (comportements propres à la tâche exécutée). CORE se base sur un composant de type watchdog **[40]** permet la surveillance des nœuds voisins, les nœuds ainsi maintiennent tout un ensemble de données sur les comportements des autres nœuds qui servent ensuite à construire des réputations directes issues des observations directes du comportement attendu d'un voisin et des réputations indirectes déduites des messages diffusés par les voisins et concernant des nœuds tiers. Les formules de combinaison de ces réputations sont fournies et l'accent est mis sur la nécessité de donner plus d'importance aux comportements passés afin de mieux tolérer les fautes passagères. Ces réputations mesurées permettent d'obtenir une valeur de réputation combinée qui sera utilisée pour décider quant à la coopération ou à l'isolation progressive d'un nœud. À noter que CORE contrairement à CONFIDANT ne permet d'attribuer que des valeurs positives pour la réputation, si le nœud de décision reçoit un rapport positif d'un autre nœud (surveillance indirecte). Les valeurs négatives sont réservées seulement pour une surveillance directe dans le cas où le nœud local surveillé ne coopère pas. En procédant ainsi, le mécanisme élimine les éventuelles fausses accusations et les attaques de dénis de service dont CONFIDANT souffre.

3.6. Conclusion

Les réseaux Ad hoc sont des réseaux dynamiques et auto-configurables sans infrastructure préexistante. Ce type de réseaux n'a pas une politique claire pour séparer les nœuds légitimes de ceux non désirés ou malicieux. Un nœud légitime ou malicieux pourrait se joindre sans distinction à un réseau Ad hoc. Ainsi, à cause de la présence des nœuds malicieux, l'un des plus grands défis dans ce type de réseaux est de proposer des solutions de sécurité robustes pouvant protéger ces réseaux contre les différentes attaques.

Nous avons pointé dans ce chapitre des vulnérabilités spécifiques aux réseaux mobiles Ad hoc. Nous les avons expliquées puis nous avons montré comment ces faiblesses peuvent être mises à profit dans la mise en œuvre d'attaques visant la confidentialité des informations transmises ou le déni de service. Ces attaques concernent, comme nous l'avons expliqué, aussi bien la couche réseau que les autres couches. Nous avons vu dans ce chapitre, une décomposition des solutions proposées qui permet de classifier les différentes solutions proposées jusqu'à maintenant. Ensuite, classe par classe, nous avons tenté de donner une idée des solutions les plus pertinentes proposées jusqu'à maintenant :

- Les solutions basées sur la cryptographie font la distinction entre les entités qui sont autorisées à prendre part au réseau (et qui sont supposées se comporter correctement) et les entités qui n'y sont pas autorisées et qui sont considérées comme étant des attaquants. Ces mécanismes souvent lourds à mettre en place, n'empêchent pas les entités ayant l'outil cryptographique nécessaire (attaquants internes) de se comporter malhonnêtement.
- Les solutions à base de systèmes de réputation font calculer par chaque nœud une opinion sur les autres entités. Cette opinion est une valeur numérique résultant de la combinaison d'observation des nœuds voisins. Les systèmes de réputation sont généralement utilisés pour détecter les entités égoïstes et les forcer à coopérer. Cependant, une entité malhonnête peut avoir une bonne réputation puisqu'elle participe aux opérations du réseau, tout en se comportant mal car elle diffuse de fausses informations. Les solutions à base de systèmes de gestion de confiance usent des propriétés intrinsèques des protocoles de routage pour chercher des incohérences entre les messages reçus. Ces solutions opèrent comme des systèmes de détection d'intrusions contre des attaquants internes.

En effet beaucoup de ces solutions ne répondent que partiellement aux exigences de sécurité imposées par la nature même des réseaux Ad hoc. C'est pourquoi, il serait intéressant, de trouver une solution qui répond aux besoins spécifique en matière des sécurisations du routage Ad hoc dont sera notre objectif dans le chapitre prochain.

Afin de trouver une solution qui soit à la fois efficace et optimale, nous nous intéressons plus particulièrement du dernier type de solutions (solutions à base de réputation et de gestion de confiance) puisque la notion de confiance est omniprésente dans les protocoles de routage Ad hoc dans lesquels les nœuds se font mutuellement confiance et se basent sur la coopération des entités. Nous nous baserons sur la confiance développée entre les différents participants du réseau pour construire un raisonnement sur le comportement de chaque entité voisine. Dans notre travail de recherche que nous présenterons dans le prochain chapitre, nous nous sommes intéressés aux problèmes de sécurité et aux attaques contre le protocole de routage AODV.

Chapitre 4. Protocole de routage basé sur la confiance et l'écoute de voisinage

4.1. Introduction

Afin que la collaboration des nœuds dans un processus de routage soit productive, le premier but des mécanismes de sécurité est d'offrir une protection contre les utilisateurs malveillants. De ce fait, il est nécessaire de donner au réseau les moyens d'inciter les nœuds à collaborer et à adopter des comportements en adéquation avec les exigences des applications. Il est nécessaire que la majorité des participants adoptent un comportement honnête. Pour cela, il est possible d'utiliser des mécanismes de protection de la vie privée qui permettent par exemple de router des messages en toute sécurité par des moyens sûrs et efficaces. Les systèmes de gestion de la confiance répondent à ce besoin. Ces systèmes tiennent une place très importante dans la littérature relative à la sécurité des réseaux ad hoc. La gestion de la confiance dans ces derniers, repose sur un modèle de réputation et/ou de recommandation qui nécessite une organisation collaborative des nœuds du réseau. Tout d'abord, les entités calculent localement leurs propres valeurs de confiance et agrègent par la suite leurs résultats.

Dans le but de traiter la sécurité, notre travail sera basé sur la gestion de la confiance appliquée au protocole de routage AODV dans les réseaux mobiles ad hoc. En ce sens, nous proposons de mettre en place un mécanisme permettant à chaque nœud participant au processus du routage de distinguer les nœuds dignes de confiance des nœuds malhonnêtes en se basant sur les observations qu'il a collecté. Ceci peut être accompli à travers l'analyse du trafic des voisins qui permet de détecter tout comportement anormal.

Dans la suite de ce chapitre avant de présenter la nouvelle architecture que nous proposons pour la détection de comportements malhonnêtes appliqué sur le protocole de routage AODV (section 4.5), nous allons essayer de donner une définition de la confiance et de la réputation telles qu'elles sont utilisées dans les systèmes de gestion de la confiance (section 4.2). Nous présentons par la suite le comportement normal du protocole AODV (aperçu sur le protocole section 4.3) en analysant la confiance implicite effectuée dans ce protocole. Nous continuons par passer en revue les attaques qu'un nœud malhonnête peut faire dans la section (4.4). Cette analyse nous permet de comprendre le comportement de l'attaquant. L'environnement de simulation, les différents paramètres de simulations ainsi que les résultats obtenus par des simulations effectuées sur la nouvelle architecture proposée seront présentés dans la section (4.6). La section finale de ce chapitre sera réservée pour la conclusion.

4.2. La notion de confiance

La confiance est le sentiment de sécurité ou la foi (la sûreté) qu'a une personne vis-à-vis de quelqu'un ou de quelque chose. C'est un concept fondamental sur lequel se base tout type de transaction, d'interaction et de communication. Quotidiennement, des mécanismes de confiance sont employés pour favoriser les relations sociales, amicales, familiales, etc.

La notion de confiance a été traitée à maintes reprises dans la littérature et une multitude de définitions est apparue. Cependant, il ne semble pas exister de définition faisant autorité, chacune abordant la confiance selon des points de vue différents qui varient selon la méthodologie utilisée pour observer le phénomène et selon le contexte dans lequel elle est employée.

- En psychologie sociale et en sociologie, la confiance est une hypothèse faite sur le futur comportement d'autrui. Il s'agit d'une conviction selon laquelle une personne serait capable d'agir d'une certaine manière face à une situation donnée : « Je vais tout raconter à mon père, j'ai confiance en ce [je suis convaincu(e)] qu'il me comprenne et m'aide » **[56]**.
- En sciences politiques, la confiance est un thème assez classique, à la fois considérée comme une des conditions d'émergence de la démocratie et comme un facteur clé de son fonctionnement **[57]**.
- Dans **[50],** selon l'auteur, la confiance est un mécanisme de coordination des échanges en situation d'ignorance ou d'incertitude : c'est elle qui permet de prendre une décision malgré l'existence d'un risque.

La thématique de la confiance informatique (numérique) est assez récente et repose principalement sur les domaines de la qualité et de la sécurité appliquées aux TIC (Technologies de l'Information et de la Communication). Dans un réseau ad hoc ouvert, un nœud compte sur la coopération de nœuds qu'il ne connait pas pour pouvoir échanger des informations. Ceci suppose de faire l'hypothèse d'accorder sa confiance aux autres et aux informations qu'ils lui présentent. La notion de confiance est ainsi interprétée comme étant l'ensemble des relations existant entre les différents utilisateurs du réseau particulièrement entre les entités participant à un protocole donné **[58]**. L'application (le protocole) détermine la sémantique de la confiance et définit la façon dont la confiance est calculée et partagée. Le mode d'évaluation de la confiance varie d'une application à une autre, tandis que la façon

d'utiliser cette confiance, afin de répondre au bon déroulement du protocole, est déterminée par les différents participants au protocole.

La notion de confiance nécessite qu'un nœud connaisse ses correspondants. Cela n'étant pas toujours possible, on peut alors mettre en œuvre une catégorie bien particulière des modèles de confiance, qui est largement utilisée dans les modèles de communication décentralisés, à savoir les systèmes basés sur la réputation ou aussi appelés les systèmes à base de recommandations : « je ne le connais pas mais des amis à moi m'ont dit qu'il était, je peux coopérer avec lui ». Cette notion va permettre au nœud de savoir s'il doit coopérer avec un tiers en se basant sur l'avis émis par d'autres nœuds de confiance **[59]**. Ces modèles offrent un mécanisme flexible et dynamique pour l'établissement de la confiance et s'appliquent bien aux systèmes distribués tel que les réseaux pair à pair (réseaux ad-hoc).

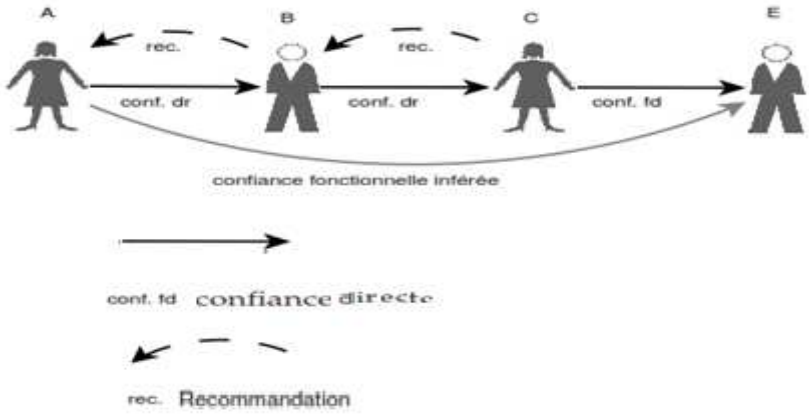

Figure 4.1. Propagation de la confiance : dans ce type de modèles, la confiance d'une entité est calculée en tenant compte, en plus du comportement et des expériences passées des entités, des recommandations qu'elles s'échangent entre elles.

4.3. Aperçu sur le protocole AODV

Dans sa forme la plus simple, AODV n'offre aucun système de sécurité. Toutes les entités peuvent participer au routage où chaque nœud est supposé se conduire correctement, impliquant ainsi une confiance implicite. Cependant, les nœuds malhonnêtes profitent de cette confiance implicite dans le protocole pour servir leurs intérêts, donc il n'y a pas de barrières pour un nœud malicieux de causer des perturbations dans le trafic circulant.

AODV est un protocole réactif, il est basé sur la construction de table de routage. En effet, chaque nœud possède sa propre table de routage contenant pour chaque destination, le prochain nœud à contacter. Le protocole AODV définit deux types d'opérations : la

découverte des routes et la maintenance des routes. La découverte d'une route se fait par inondation par l'émetteur d'un paquet RREQ (RREQ : Route REQuest). A là réception d'un de ces paquets, si le nœud connait le chemin pour accéder à la source, il envoie une réponse RREP (RREP : Route REPly) à l'émetteur qui arrête d'inonder le réseau. Si le nœud ne connait pas le chemin, il transmet le paquet à ses voisins tout en mémorisant le nœud précédent ayant fait la requête. En cas de cassure du lien, un message RERR (RERR : Route ERRor) est envoyé à l'émetteur qui décide ou non de recommencer l'envoie du paquet suivant le taux d'utilisation de la route.

4.3.1. Processus de découverte de route

4.3.1.1. Initialisation de la demande de route

Avant d'envoyer un message à la destination, le nœud source vérifie l'existence d'une route valide dans sa table de routage. Ainsi, s'il ne connait pas la destination ou s'il possède un chemin obsolète, le nœud doit initier une découverte de route. Pour ce faire, il diffuse une demande de route : RREQ<*Source_Addr, #Source_Seq, Broadcast_ID, Dest_Addr, #Dest_Seq, Hop_Count, >*

Type	J	R	G	D	U	Reserved	Hop Count
RREQ ID (Broadcast_ID)							
Destination IP Address (Dest_Addr)							
Destination Sequence Number (#Dest_Seq)							
Source IP Address (Source_Addr)							
Source Sequence Number (#Source_Seq)							

Tableau 4.1. Format de message Route REQuest (RREQ).

4.3.1.2. Propagation de la demande de route

Chaque nœud intermédiaire recevant la RREQ la retransmet après avoir effectué des mises à jour concernant le paquet RREQ ainsi que ses structures internes. Ce traitement est fait une seule fois pour une requête donnée même si cette RREQ peut être reçue plusieurs fois de différents voisins. Lors de la réception d'une demande de route RREQ, le nœud intermédiaire effectue les actions suivantes :

- il crée ou met à jour un chemin vers le nœud du quel le message est reçu selon que ce nœud appartient ou non à sa table de routage ;
- il vérifie l'existence de cette RREQ dans la table d'historique. Si elle est trouvée, le nœud traitant la supprime et arrête le traitement. Cependant, si elle n'est pas trouvée, il ajoute ou

met à jour un chemin vers la source dans sa table de routage; le nœud traitant ajoute la RREQ à la table d'historique.

- Enfin, il vérifie l'existence d'un chemin valide vers la destination dans sa table de routage. Son action dépend aussi de son positionnement : s'agit-il d'un nœud intermédiaire ou d'un nœud destination ?

(a) S'il n'est pas la destination et n'a pas de chemin valide vers la destination, il rediffuse la RREQ modifiée. La modification de la RREQ porte sur le champ nombre de saut qui est incrémenté de (1) pour compter le saut vers ce nœud traitant.

(b) Lorsqu'il n'est pas la destination mais qu'il a un chemin valide et frais vers la destination, il peut créer une RREP qu'il renvoie à la source. Le nœud traitant copie l'adresse source et destination de la RREQ vers les champs correspondants dans la RREP. Il copie ensuite la valeur du numéro de séquence qu'il a dans sa table de routage pour la destination dans le champ correspondant de la RREP et initialise le nombre de sauts à la valeur du champ nombre de sauts de l'entrée destination de la table de routage. De plus, le nœud intermédiaire effectue deux mises à jour au niveau de sa table de routage : la première concerne la liste des précurseurs de l'entrée destination à laquelle est ajouté le nœud duquel la RREQ est reçue. La seconde concerne la liste des précurseurs de l'entrée source à laquelle est ajouté le prochain saut en direction de la destination.

(c) Lorsqu'il s'agit de la destination, il copie l'adresse de la source et de la destination de la RREQ reçue dans les champs correspondant de la RREP. Ensuite, il place son numéro de séquence qui est préalablement mis à jour. Ainsi, le numéro de séquence local est incrémenté de un si la valeur reçue dans la RREQ est égale à cette valeur incrémentée. Enfin, il initialise le nombre de sauts à zéro.

4.3.2. Propagation de la réponse de route

Chaque nœud intermédiaire recevant une RREP qui le concerne (l'adresse de destination dans l'entête IP est son adresse) doit la transférer au prochain saut en direction de la source après avoir incrémenté le nombre de sauts. Le prochain saut peut être trouvé en consultant sa table de routage qu'il a construit lors du passage de la RREQ. Il est à noter qu'un nœud ne traite pas un paquet de RREP qui ne lui est pas destiné car ce message est filtré par la couche liaison. *RREP<Source_Addr, Dest_Addr, #Dest_Seq, Hop_Count, Lifetime, >*

Type	R	A	Reserved	Prefix Size	Houp count
Destination IP address (Dest_Addr)					
Destination Sequence Number (#Dest_Seq)					
Source IP address (Source_Addr)					
Life time					

Tableau 4.2. Format de message Route REPly (RREP).

Le passage de la RREP donne aussi lieu à des mises à jour de la table de routage en utilisant les informations contenues dans le paquet :

- le nœud intermédiaire met à jour l'entrée correspondante à l'émetteur du message dans sa table de routage ;
- S'il ne trouve pas d'entrée pour la destination, il l'ajoute à sa table de routage en utilisant les informations reçues dans le paquet. Lorsqu'il a déjà une entrée pour la destination dans sa table de routage, il ne la met à jour avec les nouvelles informations fraîchement reçues que dans l'un des cas suivants :
    (a) Il n'a pas de numéro de séquence valide pour l'entrée destination dans sa table de routage ;
    (b) Il ne garde que le chemin avec le plus grand numéro de séquence entre celui qui est déjà dans sa table de routage et celui reçu dans la RREP. Il s'agit en fait du chemin le plus frais ;
    (c) En cas d'égalité du numéro de séquence, il ne garde que le chemin avec le plus petit nombre de sauts. Il s'agit du chemin le plus court. Ceci est utile dans le cas où un nœud reçoit plus d'une réponse de route. Il devra alors prendre une décision qui dépend ainsi en premier lieu de la fraicheur de la route et en second lieu de la longueur de la route.
- le nœud intermédiaire recherche dans sa table de routage l'entrée à la source qui, rappelons-le, a été construite lors du passage de la demande de route pour obtenir l'adresse du prochain saut vers lequel la réponse de route est acheminée après avoir incrémenté le nombre de sauts de 1. Enfin, il met à jour les listes des précurseurs de l'entrée destination et du nœud duquel le RREP est reçue en y ajoutant le nœud vers lequel la RREP est acheminée.

4.3.3. Processus de maintient des routes

À chaque intervalle de temps, le nœud vérifie s'il a diffusé un message et si ce n'est pas le cas, il diffuse un message HELLO pour préciser aux voisins qu'il est toujours à porté radio. Les messages HELLO sont utilisés pour maintenir les informations de connectivité. À la réception d'un message HELLO, le nœud vérifie s'il a une entrée pour le voisin duquel le message est reçu dans sa table de routage pour la mettre à jour; sinon il enrichit son voisinage d'un nouveau voisin et ajoute ainsi l'entrée correspondante dans sa table de routage.

Chaque nœud contrôle aussi la connectivité des voisins. Il vérifie ainsi l'activité de ceux qui sont actifs à chaque intervalle de temps en cherchant s'ils ont envoyé un message au cours de cet intervalle. Le message peut être une notification de la couche liaison ou un message de contrôle spécifique AODV (RREQ, HELLO, . . .). Si la connectivité à un voisin ne peut pas être déterminée, le nœud doit supposer que le lien est perdu et prendre les mesures correctives nécessaires :

- Invalider les routes concernées par la perte de ce lien. Le nœud détectant la rupture d'un lien commence par marquer comme invalide le chemin vers le voisin direct dans sa table de routage ensuite tous les chemins l'utilisant comme prochain saut ;
- Créer une liste des destinations affectées contenant l'ensemble des nœuds qui ne sont plus accessibles après la rupture de ce lien ;
- Créer une liste des voisins qui devraient être informés. Pour chaque nœud de la liste des destinations affectées, prendre les nœuds se trouvant dans la liste des précurseurs, c'est à dire des nœuds qui passent par lui pour atteindre la destination ;
- Enfin, envoyer un message erreur de route RERR aux nœuds de la liste précédente.

Type	N	Reserved	Dest count
Unreachable Destination IP Address			
Unreachable Destination Sequence Number			
Additional Unreachable Destination IP Addresses (if needed)			
Additional Unreachable Destination Sequence Numbers (if needed)			

Tableau 4.3. Format de message Route ERRor (RERR).

Pour illustrer le processus AODV, le tableau 4.4 montre la séquence des étapes quand le nœud source (1) dans le réseau présenté dans la figure 4.2 essaie d'établir une route vers la destination (15). Ainsi, après avoir cherché une route valide dans sa table de routage et ne pas l'avoir trouvé, (1) initialise une demande de route (RREQ) et la browdcast dans le réseau, les

nœuds intermédiaires à leur tour browdcast le message RREQ, ou ils répondent par une RREP s'ils ont une route valide vers la destination dans leurs caches. L'identifiant de requêtes et l'identifiant de source sont utilisés ensemble pour détecter si le nœud a déjà reçu une copie de RREQ. Le nœud source peut recevoir plus d'un paquet RREP dans ce cas il va en premier déterminer quelle RREP à choisir en basant sur le nombre de saut. Chaque nœud, après avoir envoyé le paquet, va sauvegarder l'identifiant de requêtes (Broadcast_ID) et le nœud précédent (nombre de nœud précédent) depuis qui il a reçu le paquet RREQ. S'il y'a une réponse, le nœud intermédiaire sauvegarde l'identifiant de requêtes (Broadcast_ID) et le nœud précédent depuis qui il a reçu le paquet (RREP).

Etape	**Nœud**	**Action**
1	Nœud 1	Nœud source, #Source_Seq =1, #Dest_Seq = 3, Nœud destination= Nœud 15
2	Voisins du nœud 1	2, 5, 6 (aucune idée sur la destination), ainsi envoyer la RREQ aux nœuds 3, 4 et 10.
3	Nœud 4	aucune idée sur la destination.
4	Nœud 10	Il a une route vers 15 (11-14-15), le numéro de séquence de destination =4.
5	Nœud 3	Il a une route vers 15 (7-9-13-15), le numéro de séquence de destination =1.
6	Nœud 10	Répondre par une RREP, car (4>3).
	Nœud 3	Ne pas répondre (1<3) : Cela signifie que le nœud 3 a une route ancienne vers le nœud 15.
7	Nœud 4	Envoyer la (RREQ) à 12, Envoyer la (RREQ) à 15, recevoir une réponse de 15
8	Nœud 1	Va obtenir deux routes:(1-5-10-11-14-15) et (1-5-4-12-15) (1-5-4-12-15) va être sélectionnée (nombre de saut)
9	Nœud 4, 5	Rupture de lien entre 4 et 5.
10	Nœud 4	Envoie d'une RouteERRor (RRER) à 15.
11	Nœud 5	Envoie d'une (RRER) à 1.
12	Nœud 15	Supprimer l'entrée de la route à partir de sa table.
13	Nœud 1	Supprimer l'entrée de la route à partir de sa table.
14	Nœud 1	Relancer la recherche de route avec un nouvel identificateur de diffusion (id broadcast) et le numéro de séquence de destination précédent.

Tableau 4.4. AODV : Séquence des étapes pour établir une route entre (le nœud 1et le nœud15)

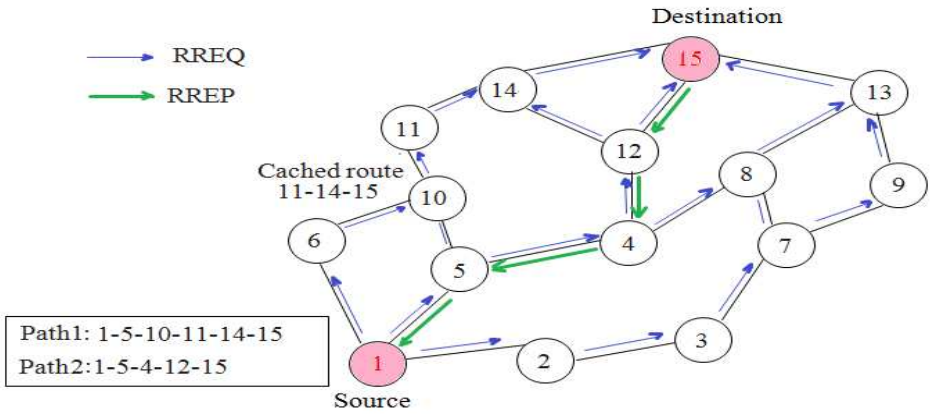

Figure 4.2. AODV : processus d'établissement de route.

4.4. Vulnérabilités du protocole de routage ad hoc AODV

L'intérêt de l'attaquant est essentiellement de nuire au bon déroulement du processus du routage pour dominer le réseau ainsi atteindre son objectif. Dans cette section, nous nous intéressons de plus près aux attaques sur le protocole de routage ad hoc AODV qui est sujet à plusieurs types d'attaques. Dans **[60]**, les auteurs étudient comment les nœuds malhonnêtes agissent sur les messages de contrôle d'AODV pour tester l'effet produit et en déduire quel objectif est atteint. Ils énumèrent quatre objectifs à savoir : (1) perturbation de route, (2) invasion de route, (3) isolation de nœud ou (4) consommation des ressources.

Pour atteindre son objectif, un attaquant se base essentiellement sur une ou plusieurs actions élémentaires. Les auteurs de cet même article classifient ainsi les actions malhonnêtes sur AODV en deux catégories : (i) atomiques, résultant de la manipulation d'un seul message de routage et (ii) composées, définies comme étant une collection d'actions atomiques. Les manipulations effectuées sur un message de routage peuvent être :

- Effacer un paquet ;
- Modifier un ou plusieurs champs du paquet avant de le retransmettre ;
- Fabriquer une réponse à la réception d'une demande de route RREQ ;
- Fabriquer activement des paquets de routage sans même avoir reçu de messages de routage.

Nous présentons, dans la suite des attaques portant sur les messages de contrôle que les nœuds malhonnêtes opèrent pour aboutir à leur objectif :

4.4.1. Suppression des messages de contrôle

Cette attaque peut paralyser le réseau complètement quand le nombre de messages supprimés augmente, les nœuds attaquants et les nœuds égoïstes peuvent tous les deux intentionnellement abandonner certains (ou tous) messages de routage et de données **[61]**.

- Un nœud malhonnête pourrait simplement effacer la demande de route reçue (RREQ). En appliquant ce genre de comportement à tout message RREQ reçu, l'attaquant ne participe pas au routage (c'est comme s'il ne fait pas partie du réseau). Une autre variante serait d'effacer sélectivement des messages RREQ (Ce comportement peut être comparé à celui d'un nœud égoïste).

- Un nœud malhonnête pourrait effacer la réponse de route reçue (RREP). Dans ce cas, la suppression de la réponse de route empêche la formation du chemin vers la destination et entraine des messages de contrôle supplémentaires suite à l'initialisation d'un nouveau processus de création de route, ce qui dégrade la qualité de service (ce type d'attaque n'a un sens que si le nœud malhonnête a été choisie sur la route reliant la source à la destination).
- Comme c'est le cas pour les RREQ et RREP, un nœud malhonnête pourrait effacer un paquet de contrôle de type RERR, en effaçant une RERR, un nœud malhonnête peut retarder la détection des liens défaillants.

4.4.2. Modification des champs des messages de contrôle

Il existe plusieurs méthodes d'attaque par modification utilisées par un nœud malhonnête, comme par exemple l'attaque de déni de service (DoS attacks) et l'attaque de trou noir (Black hole attack) **[62]**. Un nœud malhonnête peut **modifier** les demandes/réponses de route, comme il peut aussi **modifier** des erreurs de route avant de les retransmettre. À la réception d'une demande de route(RREQ) ou une réponse de route (RREP), le nœud malhonnête peut ne pas respecter la spécification pour modifier un champ qu'il a le droit de modifier comme il peut aussi **modifier** un ou plusieurs champs qu'il n'est pas supposé modifier avant de retransmettre le message. Chaque modification implique un traitement différent par exemple :

- Puisqu'un nœud n'accepte que la première copie de RREQ, en augmentant l'identifiant de la RREQ, le nœud malhonnête peut garantir l'acceptation et le traitement de la RREQ modifiée par les autres nœuds.
- Le nœud malhonnête peut jouer sur le numéro de séquence de la destination et/ou le nombre de saut dans une RREP en augmentant le premier et en diminuant le second.

Cette intervention permet de garder le chemin qui passe par le nœud malhonnête même si un autre chemin plus court est proposé par un autre nœud.

- Ainsi, avec un paquet de type RERR il peut supprimer des destinations non-joignables pour faire croire qu'elles le sont encore et ajouter des destinations qui sont joignables et actives pour faire croire qu'elles ne le sont plus et les désactiver.

4.4.3. Fabrication des messages

Les attaques par fabrication peuvent être effectuées sans avoir reçu de messages RREQ et sans pour autant être choisis sur le chemin de réponse. Un nœud malhonnête peut même fabriquer un message d'erreur de route et déclarer autant de routes non-joignables causant l'invalidation des entrées correspondantes dans la table de routage des nœuds recevant le message de contrôle.

Pour fabriquer un message, le nœud malhonnête a besoin de collecter certaines informations, en écoutant le trafic par exemple, avant d'injecter le message fabriqué. L'attaquant peut falsifier autant de champs qu'il veut pour générer son objectif:

- Un nœud malhonnête peut par exemple provoquer l'inondation du réseau par des messages de routage inutiles par envoie répétitif de paquet RREQ (Le nœud malhonnête peut orienter le trafic vers une seule destination.)
- À la réception d'une RREQ, le nœud malhonnête fabrique une réponse de route même s'il n'a pas de chemin valide vers la destination. un attaquant peut même fabriquer et injecter des réponses de routes dans le réseau, même sans avoir reçu une demande de route au préalable pour but de déborder la table de routage d'une cible en proposant des routes vers des nœuds nouveaux ou inexistants ou pour proposer un chemin plus court et plus frais provoquant la mise à jour du chemin vers la destination qui passe dorénavant par ce nœud malveillant.

4.4.4. Attaque de trou noir (Black hole attack)

Dans cette attaque, Le nœud malveillant trompe tous ses voisins pour attirer tous les paquets de routage vers lui **[63]**. Un seul attaquant peut menacer l'ensemble de ses nœuds voisins. Il exploite le protocole de routage ad hoc (ici AODV) pour annoncer des routes optimales qui passent par lui : Apres la réception d'une RREQ (Route REQuest), l'attaquant unicast un faux message RREP (Route REPly) au nœud source (pour annoncer qu'il est la

voie la plus optimale pour la destination demandée). Lorsque le nœud source reçoit le message RREP fabriqué, il met à jour sa route vers le nœud destination à travers le nœud malveillant (voire la figure 4.3). L'attaquant absorbe les paquets qu'il a reçus depuis la source sans les transmettre à la destination.

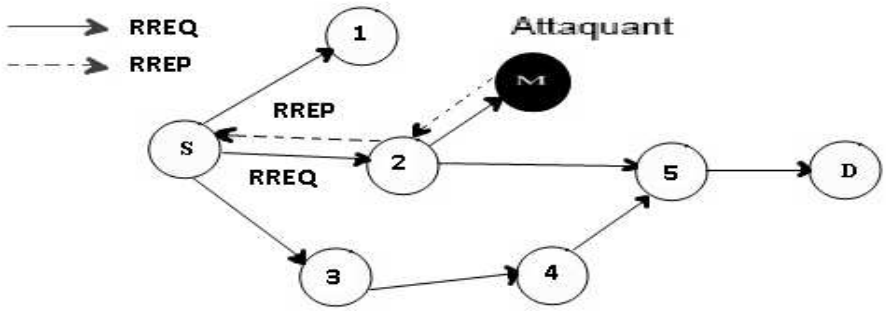

Figure 4.3. Black hole attack.

4.4.5. Rushing d'une demande de route

Dans d'autres cas, comme nous avons déjà parlé dans le chapitre précédent (section 3.4.2.8), le nœud malhonnête peut utiliser la technique du **rushing** pour nuire au bon déroulement du processus AODV. Cette attaque consiste à diminuer le temps de traitement des messages RREQ et les retransmettre plus rapidement de telle sorte qu'ils atteignent plus rapidement la destination. Ceci garantira pour le nœud malhonnête une place sur le chemin.

4.4.6. Le rejeu de messages

Un nœud malicieux réinjecte des messages dans le réseau **[64]**. Des anciens messages continuent à circuler ce qui occupe la bande passante inutilement et peut même affecter la justesse des informations concernant la topologie du réseau. Les auteurs dans **[65]** ont considéré l'attaque de type de trou de ver comme un type de cette attaque.

4.4.7. Attaque de trou de vers (wormhole attack)

Dans l'attaque du trou de ver **[65]**, un nœud compromis dans le réseau collabore avec un attaquant externe pour créer un tunnel dans le réseau. Les attaquants peuvent tromper le nœud source pour gagner dans le processus de découverte de route et plus tard lancer leurs attaques. À travers ce tunnel ils envoient directement une RREQ à la destination demandée. Les paquets de ces deux attaquants sont généralement transmis par connexion filaire pour créer l'itinéraire le plus rapide de la source vers la destination. De ce fait, ils peuvent empêcher de façon permanente d'autres voies d'être établies.

4.4.8. Usurpation d'identité

Consiste à se faire passer pour quelqu'un d'autre en utilisant son identité. L'attaquant se présente en utilisant l'identité d'un nœud légitime et peut ainsi communiquer avec les nœuds du réseau sans être rejeté.

Le tableau 4.5 résume des conséquences des attaques possibles affectant les paquets de contrôle du protocole étudié AODV.

Champ	**Est modifiable ?**	**Attaque**
Type	Non	- Changer le type : Rejeu du message (non conforme au type déclaré)
Id_source	Non	- Changer Adresse source : Fausser la découverte de route (trafic inutile). - Fabriquer un message avec l'identité d'un nœud légitime.
Id_destination	Non	- Changer Adresse destination : Rediriger le paquet ainsi l'attaquant crée des routes vers des destinations inexistantes pour consommer l'énergie du réseau (trafic inutile : déni de service).
Id_Broadcast	Non	Ce champ permet d'identifier la requête d'une manière unique et de supprimer une demande déjà traitée. - L'adversaire incrémente l'identifiant (dans une RREQ) pour rendre la RREQ acceptable (plus fraiche) pour invalider toute les futures requêtes venant d'un nœud légitime. - Décrémenter ce champ dans une requête valide pour rendre la RREQ non-acceptable ainsi empêcher la mise à jour de la table de routage des nœuds intermédiaires car la requête sera considérée comme une demande déjà traitée.
Nbr_saut	Oui (autorisé +1)	- L'adversaire incrémente ce champ : a) dans une RREQ pour ralentir la découverte de route b) dans une RREP pour fausser le nombre de sauts vers la destination. - Décrémenter ce champ : a) dans une RREQ pour mettre à jour le chemin inverse vers la source b) dans une RREP pour fausser le nombre de sauts vers la destination. Le plus souvent quand le nœud malicieux reçoit un paquet, il suffit qu'il positionne le nombre de saut à 0 pour se présenter comme relai à faible coût.
Num de seq	(Non) pour num de sequence de la source (Possible) pour num de séquence de destination	Un numéro de séquence élevé force la mise à jour au niveau des nœuds récepteurs du paquet. En manipulant ce champ l'adversaire peut injecter de fausses informations de topologie. Par exemple : - L'adversaire incrémente le Num de seq Source pour mettre à jour le chemin inverse vers la source et peut le décrémenter pour ne pas mettre à jour le chemin vers la source. - Il incrémente le Num de seq Destination pour forcer à garder le chemin avec le plus grand numéro de séquence et le décrémente pour diminuer les chances (en cas de RREP multiples).

Tableau 4.5 attaques possibles affectant les paquets de contrôle du protocole AODV.

4.5. Nouvelle architecture proposée : Détection des nœuds malhonnêtes avec un raisonnement basé sur la confiance et l'écoute du voisinage commun

AODV tel que spécifié n'offre aucun système de sécurité où chaque nœud est supposé se conduire correctement, impliquant ainsi une confiance implicite, en outre AODV ne garde pas assez d'informations pour vérifier les comportements des voisins. Par conséquent, pour combler ces problèmes, nous proposons de modifier le protocole de routage AODV en un protocole de routage plus sécurisé basé sur la notion de confiance et l'écoute de voisinage commun: Nous nous intéressons dans cette solution à la détection des comportements malveillants en se basant sur les observations des nœuds voisins. Un nœud voisin peut ainsi écouter un autre voisin, il peut détecter qu'il a reçu un message, comme il peut écouter s'il va l'émettre ou non aux autres nœuds dans le réseau. Cette proposition permet ainsi d'enrichir la connaissance de chaque nœud en stockant des informations additionnelles lui permettant de décider de l'honnêteté du voisin.

La notion de confiance est interprétée comme étant l'ensemble des relations existant entre les différents utilisateurs du réseau. Cette technique repose sur l'hypothèse de la coopération entre les nœuds qui améliore considérablement le facteur de confiance sur les nœuds voisins dans le réseau. Le niveau de confiance des entités participant au protocole de routage est ainsi utilisé pour sélectionner le chemin le plus de confiance plutôt que de choisir le plus court chemin en nombre de sauts entre un nœud source et une destination.

Le mécanisme de l'écoute de voisinage permet de diviser le réseau ad hoc en plusieurs zones auto-organisées pour en faciliter la surveillance et la gestion de confiance (voir figure 4.4). Un nœud de confiance tout seul ne peut pas former son propre groupe, il doit avoir au moins un nœud voisin de confiance. C'est le nœud avec la plus grande valeur de confiance dans la zone de voisinage commun qui va écouter les nouds voisins qui ont une valeur de confiance faible. Pour le bon déroulement du mécanisme de l'écoute de voisinage commun on propose :

- qu'au départ (au début de construction du réseau), les nœuds légitimes se connaissent entre eux (c-à-d valeur de confiance très élevée « 1 »).
- Pendant cette phase les nœuds procèdent à la connaissance de leurs voisins (échange de paquet HELLO).
- Deux nœuds différents appartient au réseau ont au moins un voisin commun.

- Une hypothèse d'absence de mobilité pendant la formation de liste de voisins communs doit être vérifiée.
- Une synchronisation entre les nœuds supposés fixes au cours de cette étape est nécessaire pour le bon déroulement du protocole de routage.
- Pas de collisions dans le système.
- L'établissement de liste de voisinage commun est répété périodiquement, suite aux changements de la topologie qui peuvent suivre.

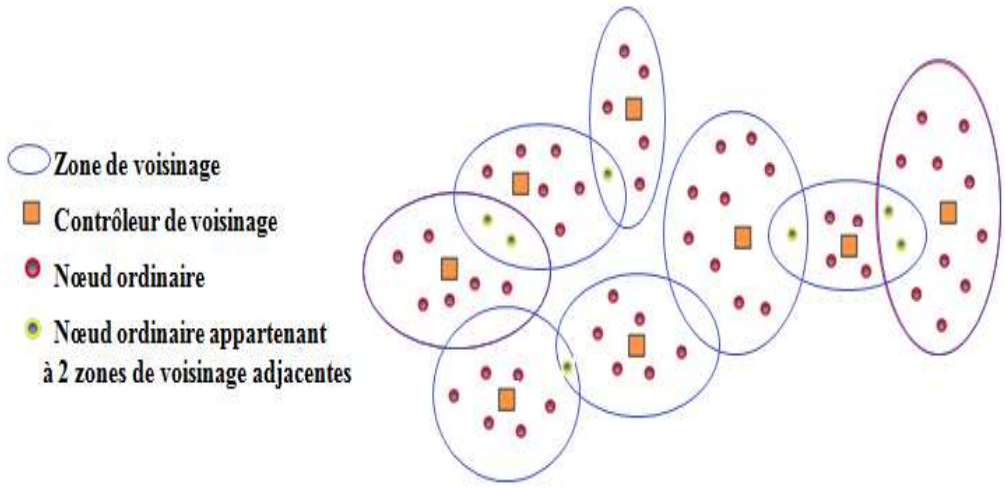

Figure 4.4. La décomposition du réseau en zones de voisinage commun auto-organisées (sous Trust AODV).

Notre proposition est formulé sous un protocole doté (Trust AODV) qui est fondamentalement une extension du protocole AODV pour améliore le niveau de sécurité AODV et aussi de prévenir une attaque de nœud malveillant dans le réseau. Ce raisonnement repose sur un ensemble de contrôles, dans les sections suivantes, nous allons présenter les concepts de notre protocole (Trust AODV).

4.5.1. Etablissement de la liste de voisinage commun

Pour réaliser ce protocole on a besoin de définir pour chaque deux nœuds différents appartient au réseau une liste (table) de voisinage commun.

Processus « **Etablissement de la liste de voisins communs »**

Début

A, B, C trois nœuds du réseau.

Si (C voisin directe de A et C voisin directe de B) **alors**

- Entrer C dans la liste de voisins communs de A et B

Fin

Nb: voisin directe c-à-d la distance entre les deux nœuds = 1saut.

Dans l'image en dessous (Figure 4.5): Les nœuds A, B ont comme voisins communs les nœuds {1, 2}, de même Les nœuds B, C ont comme voisins communs les nœuds {3, 4, 5}.

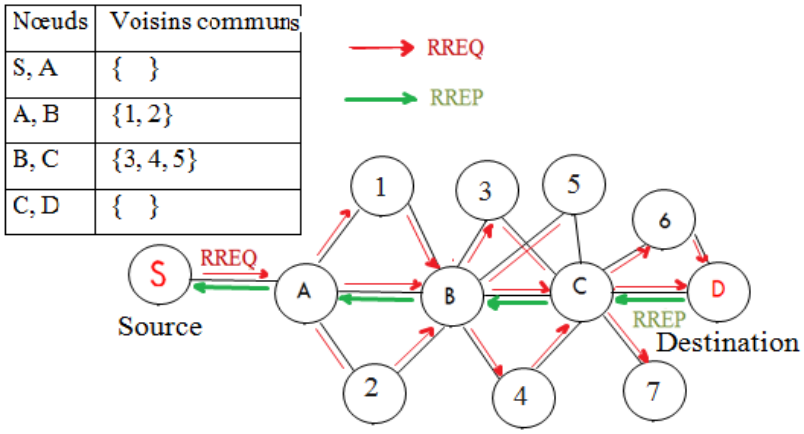

Figure 4.5. Mécanisme de sécurité par voisinage commun (établissement de la liste du voisinage commun).

Les membres de cette liste de voisinage vont contrôler les voisins soupçonnés ou inconnus en utilisant le mécanisme d'écoute pour détecter les comportements anormaux des voisins. Nous supposons qu'il existe un système de surveillance comme un watchdog (voir chapitre3 section 3.5.3.1.1) pour surveiller des nœuds voisins et d'informer les autres nœuds sur ceux qui ont des mauvais comportements. En plus les nœuds sont affectés des valeurs de confiance basées sur ces surveillances. Par conséquent, les nœuds peuvent avoir des valeurs de confiance différentes.

Ce système surveille la circulation du trafic dans le réseau (voisinage). On assume que toutes les activités d'un voisin peuvent être surveillées ainsi tout comportement anormal peut être identifié. Si un nœud mobile (surveilant) découvre une éventuelle attaque par un intrus: il

avise tous les autres nœuds du voisinage de la présence d'une attaque par la diffusion d'un message d'alarme, le système isole ainsi le nœud particulier en interdisant sa participation dans le réseau. Le processus de recherche d'une route sera refait par des nœuds voisins du nœud malicieux détecté et pas depuis le nœud source (gain du temps).

Le processus de contrôle est résumé dans l'algorithme suivant :

La procédure d'écoute de voisin

Début

Liste noire : liste des intrus détectés, (trust value = -1).

Liste (vc) : liste de voisinage commun.

Moniteur : nœud contrôleur appartient à la liste (vc), (trust value = 1).

Contrôlé : nœud contrôlé dans la liste (vc), (trust value < 1).

Step1 : **Moniteur** écoute le trafic.

Si (un **Contrôlé** a envoyé un paquet dans la zone de voisinage) **alors**

- Aller au **Step 2.**

Si (un **Contrôlé** a reçu un paquet dans la zone de voisinage) **alors**

- Aller au **Step 3.**

Step2 : **Si** (destination du paquet reçu appartient **Liste (vc)**) **alors**

- Continuer à écouter le trafic.

Sinon c'est une attaque de trou de ver.

- Aller au **Step 4.**

Step3 : **Si** (un **Contrôlé** a envoyé un paquet dans la zone de voisinage) **alors**

- Aller au **Step 2.**

Sinon c'est une attaque de trou noir.

- Aller au **Step 4.**

Step4 :

- Ajouter Contrôlé à la Liste noire.
- Supprimer toute les routes passant par lui dans la table de routage.
- Informer tous les nœuds qui appartiennent à la **Liste (vc).**
- Refaire le processus de la recherche de la route.

Fin

4.5.2. Principe du protocole Trust AODV

La confiance est établie entre deux entités participant à un protocole par rapport à une action spécifique. Elle nécessite qu'un nœud connaisse ses correspondants. Cela n'étant pas toujours possible. Dans ce protocole la confiance sur un nœud spécifique (inconnu ou avec une valeur de confiance minimale) est calculée en utilisant les opinions des autres nœuds de confiance (principe de réputation et de recommandation).

A titre d'exemple, quand un nœud (A) veut faire confiance à un autre nœud (B), le nœud A vérifie d'abord sa propre table de confiance. Si le nœud B se trouve dans sa table et la valeur est «favorable» (voir le tableau 4.6), alors B peut être un nœud de confiance «digne de confiance», si la valeur est « défavorable », B ne peut pas être un nœud de confiance.

Tant que la valeur de confiance d'une entité dans la table de confiance est égale à (1), elle se voit attribuer un niveau «favorable», qui signifie «digne de confiance», sinon, elle se voit attribuer un niveau «défavorable», ce qui signifie "non digne de confiance ". Au début, tous les nœuds peuvent être de confiance.

Nœud	Valeur de confiance (trustvalue)	Opinion de A sur B
A	1	Honnête
B	1	Honnête (favorable)
	0 < t < 1	?
	-1	Malhonnête (défavorable)

Tableau 4.6. La relation de confiance sous le protocole Trust AODV.

Chaque nœud a une liste d'estimation qui conserve des valeurs de confiance des autres nœuds et qui est actualisée à chaque changement. Une valeur de confiance est mise à jour à chaque communication réussie. Cette valeur sera incrémentée si le comportement d'un nœud est normal et elle sera décrémentée autrement.

Le protocole ajoute également deux nouveaux champs dans la table de routage AODV, la l'accumulateur de valeurs de confiance (Sum [t]) et le meilleur chemin (Bp). Notre protocole va renforcer le mécanisme de sécurité à l'aide des champs supplémentaire dans le format de requête/réponse de route. Il étend les messages de routage fondamentaux d'AODV qui sont la RREQ (Demande de routage) et la RREP (Réponse de routage) en ajoutant des champs d'information de confiance. Il propose ainsi une solution adéquate en vérifiant les messages T-RREQ (Trust RREQ), T-RREP (Trust RREP) des nœuds adjacents pour les activités

d'intrusion possibles. Chaque nœud dans le chemin, vérifie la T-RREQ/T-RREP diffusée depuis son voisin direct pour voir s'il a fourni la bonne information dans le champ supplémentaire de niveau de confiance (favorable ou défavorable). Quand un nœud intermédiaire reçoit la T-RREQ/ T-RREP il modifie le champ niveau de confiance par inclure son propre niveau de confiance, ainsi qu'il ajoute sa propre valeur de confiance à l'accumulateur de confiance (Sum [t]) dans le champ correspondant des messages de découverte de route. Chaque nœud met également à jour sa table de routage avec toutes les informations contenues dans les messages de contrôle.

Chaque nœud peut diffuser ces messages à ses voisins avec une grande fiabilité (sureté), puis il calcule de bout en bout un chemin sécurisé sans des nœuds malveillants grâce à la collaboration de nœuds dans le chemin. La sélection d'itinéraire est effectuée pendant le cycle de découverte de route en utilisant le niveau de confiance. Le meilleur chemin (Bp) basée sur la confiance et le nombre de sauts (une route sécurisé avec un nombre minimum de sauts) entre la source et la destination.

Dans le cas où le nœud adjacent obtenu une T-RERR (Trust RERR), le nœud adjacent vient d'enquêter sur l'honnêteté de l'émetteur dans le voisinage à travers l'envoi de message de contrôle.

4.5.2.1. La découverte de route (Route Discovery)

Le nœud source diffuse un message de découverte de route (T-RREQ) à ses voisins, qui contient:

T-RREQ <Source_Addr, #Source_Seq, Broadcast_ID, Dest_Addr, #Dest_Seq, Hop_Count, Sum[t], Bp>

Comme les messages RREQ dans AODV, pour trust AODV, quand les messages T-RREQ sont diffusés, chaque nœud intermédiaire reçoit ce message, il met en place un chemin inverse vers la source tout en enregistrant le voisin à partir du quel il a reçu la T-RREQ.

Pendant ce temps, lorsque le nœud reçoit la T-RREQ, il va vérifier si il est la destination ou non, si oui, il met à jour la table de routage pour ce nœud et génère une réponse de route T-RREP. Mais si le nœud récepteur est un nœud intermédiaire qui n'a pas de route vers la destination, il transmet le paquet T-RREQ après avoir ajouté sa valeur de confiance dans sa table de routage au champ correspondant et après l'avoir attaché à l'accumulateur de valeurs de confiance Sum [t] dans le message qui est calculé par :

$$Sum[t] = \sum_{i=1}^{n} trust_{value}(i) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Avec :

n : nombre total de sauts reçu dans une route.

Sum[t]: l'accumulateur de valeurs de confiance.

$trust_{value}$ (i): valeur de confiance du nœud voisin dans la table de routage.

Ainsi, à n'importe quel moment, le paquet T-RREQ contient une liste de tous les nœuds visités avec leur valeur de confiance ajouté à l'accumulateur de valeurs de confiance Sum[t], la valeur de confiance du voisin à partir du quel le message a été reçu et la valeur du meilleur chemin (Bp) pour les nœuds intermédiaires) depuis la source.

Chaque fois qu'un nœud reçoit un paquet T-RREQ, un nœud va vérifier les mises à jour de chemin vers le nœud source. Il compare alors la valeur du meilleur chemin (Bp) dans la table de routage avec la nouvelle valeur du meilleur chemin (Bp) associé au message, si la nouvelle (Bp) est supérieure à celle de la table de routage, le nœud met à jour la table de routage. Cette valeur est calculé par :

$$Best\ Path\ (Bp) = \frac{Sum[t]}{\sqrt{Hop_{count} * Hop_{count}}} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Avec :

Best Path (Bp) : le meilleur chemin basé sur la valeur de confiance et un nombre moins de sauts.

Hop_{count}: nombre de sauts inclus dans une T-RREQ.

Une nouvelle entrée est créée dans la table de routage pour tous les nœuds intermédiaires, s'ils n'ont pas de valeur de confiance alors une valeur de confiance propre à chacun d'eux sera attribuée. Si une entrée de route pour un nœud existe, et si le meilleur chemin (Bp) d'un nœud intermédiaires quelconque est plus grand que le meilleur chemin connu précédemment de ce nœud, l'entrée de la table de routage est mise à jour pour ce nœud et lui assigne une nouvelle valeur de confiance calculé à partir de l'accumulateur de valeurs de confiance Sum [t] et le nombre de sauts de la route Hop_{count} :

$$trust_{new_{value}} = \frac{Sum[t] - 0.1}{Hop_{count}} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

Où:

Trust $_{new\_value}$: la nouvelle valeur de confiance qui va être modifiée dans la table de routage.

4.5.2.2. La réponse de route (Route Reply)

Après la réception de la T-RREQ, le nœud destination crée un message de réponse de route (T-RREP) et envoi en unicast ce message à la source sur le chemin inverse. Un message T-RREQ contient les champs suivants:

T-RREP<Source_Addr, Dest_Addr, #Dest_Seq, Hop_Count, Lifetime, trustvalue, Sum[t], Bp>

Quand le message T-RREP est unicast vers la source, chaque nœud intermédiaire transmet ce paquet en ajoutant sa valeur de confiance au champ de l'accumulateur de confiance Sum[t] dans le paquet. Semblablement à la T-RREQ, la table de routage est mis à jour pour chaque nœud intermédiaire visité par le T-RREP en plus au nœud de destination. Conformément à AODV, les entrées sont également créées dans les listes de précurseurs par un nœud transmettant une réponse de retour vers la source.

4.6. Simulations et résultats : Expérimentation du raisonnement basé sur la confiance et l'écoute du voisinage

Nous avons effectué les simulations sur le simulateur réseau NS-2. Dans cette section, nous allons premièrement présenter l'environnement de simulation NS-2 sur lequel on va implémenter notre protocole trust AODV proposé comme extension du protocole AODV. Enfin, après avoir décrit les différents paramètres à prendre en considération pour mettre en place la simulation, nous montrons l'efficacité de la solution à travers les résultats obtenus de simulation.

4.6.1. Environnement de simulation

Malgré la présence de plusieurs simulateurs de réseau tels que GloMoSim, OMNET et OPNET, NS-2 **[66]** (Network Simulator version 2) reste le simulateur de réseau le plus utilisé dans le milieu académique ainsi que dans l'industrie. Il est considéré par beaucoup de spécialistes des télécommunications comme le meilleur logiciel de simulation par événements discrets, en raison de son modèle libre, permettant l'ajout très rapide de modèles correspondant à des technologies émergentes **[67]**.

NS-2 fournit un environnement assez détaillé permettant entre autre de réaliser des simulations d'IP, TCP, du routage et des protocoles multicast aussi bien sur des liens filaires que sans fil. C'est un outil de recherche très utile pour le design et la compréhension des protocoles, permet à l'utilisateur de définir un réseau et de simuler les communications entre les nœuds de ce réseau. Il fournit les mécanismes nécessaires à la mise en œuvre des protocoles et la simulation de leurs comportements. Il est principalement bâti avec les idées de la conception par objets, de réutilisabilité du code et de modularité. Il est devenu aujourd'hui un standard de référence en ce domaine.

NS-2 combine le langage de script OTcl et le langage C++. L'interpréteur OTcl (Object Tools Command Language) dérivé du langage TCL sert à exécuter les scripts de commande utilisateur qui permettent la configuration, la description et la mise en place des simulations. Dans le script l'utilisateur fournit la topologie du réseau, les caractéristiques des liens physiques, les protocoles utilisés, le type de trafic généré par les sources, les événements, etc. alors que C++ est utilisé pour l'implémentation du noyau du simulateur ainsi que des protocoles. L'écriture des routines en C++ permet d'avoir une plus grande puissance de calculs.

Le résultat d'une simulation est un fichier texte contenant tous les événements de la simulation. Un traitement ultérieur de ce fichier permet d'en soustraire l'information souhaitée. Par ailleurs, le simulateur permet la création d'un fichier d'animation (d'extension .tr), permettant de visualiser la simulation sur l'interface graphique NAM. Cette visualisation fournit une représentation du graphe du réseau sur laquelle on peut voir les paquets circuler, suivre le niveau des files d'attente et observer le débit courant des liaisons.

NS-2 est fourni sous forme d'un paquetage qui regroupe tous les fichiers nécessaires à son installation. Il est conçu initialement pour fonctionner sur les systèmes d'exploitation Unix et Linux, mais il existe un moyen pour son installation sur un système Windows 2000/XP; il s'agit de l'émulateur Cygwin qui offre un environnement Linux sous Windows. L'utilisation du simulateur NS-2 est gratuite, il est disponible dans le domaine public d'Internet sur le site http://www.isi.edu/nsnam/. On le trouve sous le nom : ns-allinone-version.tar.gz. Dans nos simulations, nous avons utilisé la version ns-allinone-2.34 sous la plateforme LINUX ubuntu-10.10-desktop-i386-fr.

NS-2 sert aussi bien dans l'étude des protocoles de routage dans les réseaux mobiles. Par conséquent on trouve que le protocole AODV est directement géré par NS-2 parce que son implémentation est inclue par défaut dans NS-2, donc c'est très simple à mettre en place.

4.6.2. Mise en place des simulations dans NS-2

Nous présentons ici les différents paramètres à prendre en considération dans les simulations. Ces paramètres sont initialisés dans le script (<nom_script.tcl>). Nous décrivons ainsi le contenu de ce fichier regroupant les paramètres des simulations qui concernent la topologie, le trafic, la mobilité, le timing des événements, etc.

a) **La topologie :** Nous considérons un réseau ad hoc composé de 40 nœuds mobiles placés au hasard sur un terrain dégagé de 500 m × 500 m. Les nœuds utilisent le protocole MAC IEEE 802.11.

b) **La structure des nœuds :** Chaque nœud maintient une file d'attente de type FIFO (first in, first out). Ainsi, les messages les plus anciens sont effacés lors d'un débordement dans cette file.

c) **La mobilité :** Les nœuds se déplacent constamment en utilisant le modèle de cheminement random waypoint, c'est un scénario de mouvement généré aléatoirement et les nœuds se déplacent linéairement avec une vitesse constante comprise entre 0.0 et 20.0 m/s de sa position jusqu'à la destination choisie.

d) **Le modèle du trafic :** Chaque simulation dure 100 secondes durant laquelle un certain nombre de pairs de nœuds veulent échanger des paquets de données de type CBR (Constant Bit Rate). La taille des paquets échangés est de 512 octets.

Le tableau 4.6 présente les différents paramètres utilisés dans les simulations.

Nombre de nœuds	40
Temps de simulation	100 seconds
Dimension du terrain	500 m x 500 m
Modèle de mobilité	Random waypoint
Protocole MAC	IEEE 802.11
Modèle du trafic	CBR
Nombre de paires (source, destination)	4
Nombre de nœuds malhonnêtes	5

Tableau 4.7. Les paramètres de simulation.

Une fois que les scripts de simulations ainsi que les fichiers contenant les scénarios de mobilité et de trafic sont prêts (l'utilitaire ./setdest de NS-2 est le générateur aléatoire de scénarios de mobilité des nœuds et l'utilitaire ./cbrgen est le générateur des modèles de trafic aléatoire), il suffit de le lancer les simulations. Une fois l'exécution des simulations terminée, nous analysons les fichiers de trace en utilisant des scripts awk et les résultats obtenues sont présenter sous forme de courbes à l'aide du programme Excel. Dans la section suivante, nous présentons ces courbes et nous interprétons leur signification.

4.6.3. Résultats des simulations

Pour pouvoir analyser les performances du protocole, nous nous basons sur le calcul des trois métriques :

- **Le Taux de paquets reçus avec succès** : C'est le nombre de paquets de données reçus avec succès par la destination par rapport au nombre de paquets de données émis par la source.
- **Le Délai de bout-en-bout** : C'est le temps moyen qu'un paquet de données envoyé avec succès prend pour atteindre la destination.
- **Le Débit de routage** : c'est la quantité d'information transmise par unité du temps.

Ces métriques seront exécutées sur le protocole trust AODV auquel nous avons ajouté notre système de détection et le protocole de base (AODV sans modification). Cela nous permet de faire une comparaison entre les performances obtenues par les deux protocoles. Ainsi, pour chaque métrique, nous avons réalisé des simulations pour trois cas de figures différents :

- **Cas 1 :** Exécution du protocole AODV sans aucune modification et sans attaque.
- **Cas 2 :** Exécution du protocole AODV sans aucune modification et avec attaque (ici on a utilisé l'attaque Black hole). Les courbes correspondantes sont notées « BAODV : Blackhole AODV».
- **Cas 3 :** Exécution du protocole trust AODV auquel nous avons ajouté notre système de détection avec attaque. Les courbes correspondantes sont notées « TRUST AODV».

Dans ce qui suit nous allons faire des interprétations des résultats obtenus après l'exécution de ces métriques dans les différents cas 1, 2 et 3.

4.6.3.1. Taux de paquets reçus avec succès (PDR : Packet Delivery Ratio)

Dans la figure 4.6, le taux PDR pour l'exécution du protocole AODV modifié ‘‘Trust AODV ’’avec attaque montre un taux de paquets délivrés avec succès supérieur par rapport AODV non modifié en présence d'attaque qui montre les plus faibles taux de paquets délivrés avec succès. Ceci est logique puisque dans ces expérimentations nous avons mis en place des attaquants perturbant les opérations de routage ce qui explique la dégradation de ce taux.

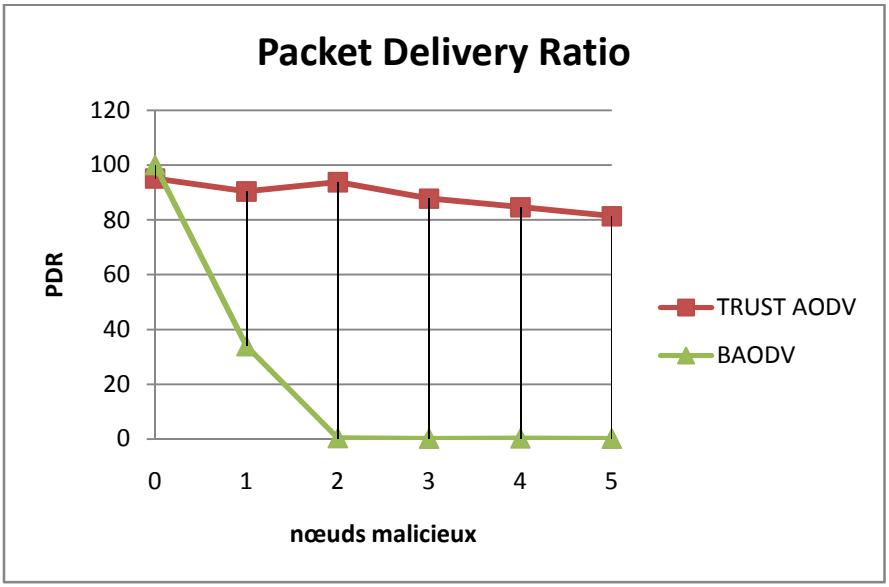

Figure 4.6. Packet Delivery Ratio Vs nombre des nœuds malicieux.

La cause que le taux de Trust AODV est meilleur à celui de AODV normal en présence d'attaque est expliqué par le principe que Trust AODV pour envoyer le trafic, se base sur les nœuds digne de confiance en dépendance de la technique qui consiste à choisir le meilleur chemin (BP) entre la source et la destination (la route la plus sécurisée et la plus fraiche avec le petit nombre de saut possible), l'utilisation d'une route sécurisée réduit la probabilité de rupture de route à cause de suppression de message par un attaquant. De ce fait, le nombre de paquets perdu avec Trust AODV est beaucoup mois que celui perdu avec AODV sans modification et en présence d'attaque.

4.6.3.2. Délai de bout-en-bout (EED : End-to-End Delay)

Ce temps inclut le délai de traitement ainsi que le délai d'attente dans les files d'attentes dans chaque nœud intermédiaire. La figure 4.7 montre l'évolution de ce temps en fonction du nombre de nœuds malicieux dans le réseau. Nous remarquons l'alternance des valeurs obtenues : une dégradation est constatée dans le taux relatif à Trust AODV par rapport au protocole AODV original sans attaque quand le nombre des nœuds malveillants est égal à

zéro. Cependant notre proposition dégage une amélioration très importante par rapport à BAODV (c.à.d. AODV original en présence d'attaque), ceci revient essentiellement au fait que l'attaquant continu à participer normalement aux opérations de routage après avoir exécuté son action malhonnête, ce qui contribue à diminuer le délai de bout en bout. Trust AODV a marqué cette amélioration grâce à son mécanisme du meilleur chemin qui sélectionne la route de confiance pour l'envoi des données.

Ceci montre que l'implémentation du système de détection que nous proposons n'influe pas sur le traitement des paquets et n'engendre pas de temps de traitement supplémentaires ralentissant le déroulement normal du protocole.

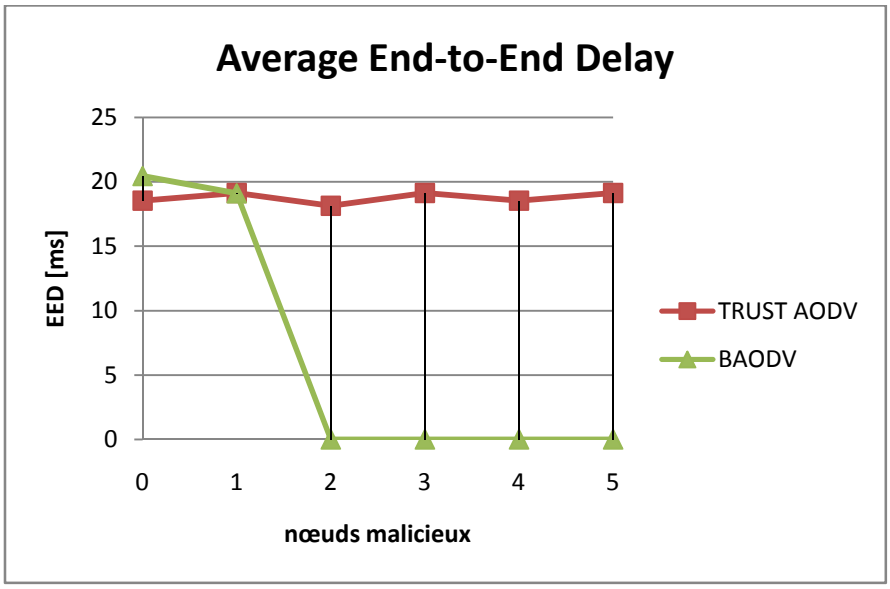

Figure 4.7. End-to-End Delay Vs nombre des nœuds malicieux.

4.6.3.3. Le Débit de routage

La figure 4.8 montre que le débit est réduit lorsque le réseau est attaqué. Le débit est meilleur quand le nombre de nœuds malveillant est égal à zéro avec le protocole d'origine AODV. Par contre, pour le protocole BAODV va rapidement vers le zéro en augmentant le nombre de nœuds malicieux. Le débit est de toute évidence augmenté pour Trust AODV (AODV avec le mécanisme de l'écoute du voisinage commun). Ainsi, nous démontrons que le système de détection d'actions malhonnêtes est efficace sans pour autant toucher aux performances du protocole : il permet d'ajouter une ligne de défense supplémentaire au protocole AODV.

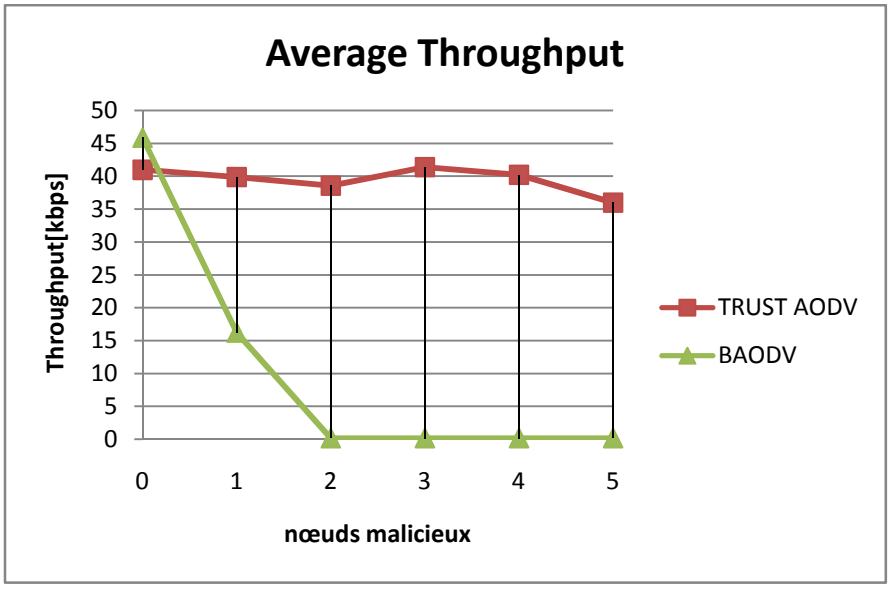

Figure 4.8. Average Throughput Vs nombre des nœuds malicieux.

4.7. Conclusion

Nous avons vu dans ce chapitre qu'AODV tel que conçu ne suppose aucun mécanisme de sécurité, toutes les entités peuvent participer au routage où chaque nœud est supposé se conduire correctement, impliquant ainsi une confiance implicite. Cette spécification d'AODV le rond très vulnérable et les nœuds malhonnêtes exploitent la confiance aveugle que les nœuds développent envers leur voisinage pour réalise leurs objectifs. L'objectif principal d'un nœud malicieux est de perturber le protocole de routage. Par conséquent, rendre le routage plus sécurisé est un aspect très important pour des réseaux comme les MANETs.

Dans ce chapitre, nous avons proposé un nouvel algorithme de routage doté Trust AODV qui est fondamentalement une extension du protocole réactif AODV. Notre algorithme constitue d'un système de gestion de confiance pour renforcer la sécurité ainsi qu'un autre système de contrôle et d'évaluation de la confiance entre les différents participant du réseau basé sur la surveillance du voisinage.

Nous avons mené une série de simulations afin d'évaluer les performances de notre algorithme proposé. Nous avons utilisé pour cela le simulateur NS-2, dans lequel nous avons fait l'implémentation de l'algorithme proposé. Durant les simulations utilisées, chaque nœud est affecté une valeur de confiance. Avec l'inclusion de notre système de détection basée sur la confiance et l'écoute de voisinage, la valeur de confiance est mise à jour selon le résultat de surveillance ainsi que les relations d'interaction du nœud avec les membres des nœuds appartenant à la même zone de voisinage que lui.

Pour tester la résistance de notre modèle de détection, nous avons mis en place quelques exemples d'attaques. Cela nous a permis de faire une comparaison entre les performances obtenues par les deux protocoles (le protocole Trust AODV proposé et AODV sans modification) pour montrer que notre système peut réaliser un niveau considérable de sécurité sans qu'il dégrade beaucoup les qualités du système.

La comparaison des courbes obtenues à l'issue de l'exécution du trois cas (AODV sans modification avec absence d'attaque, AODV sans modification avec présence d'attaque et Trust AODV avec présence d'attaque) montre que l'ajout de notre système de détection n'influe pas beaucoup sur les performances du protocole de base, tout en rendant le routage plus sûr.

Pour délivrer les données notre protocole Trust AODV choisi les meilleurs chemins (Bp) basant sur la route la plus sûr (de confiance) avec un nombre minimale de saut entre la source et la destination. Durant la simulation Trust AODV a marqué un grand pourcentage de succès pour la livraison des données aux destinations demandées par rapport au protocole AODV sans modification en présence d'attaque. Cependant, il est probable que due à extra traitement dans certaines situations et avec la possibilité que les paquets peuvent suivent des routes très longues, est aussi présenté avec notre protocole proposé qui va augmenter le délai de bout en bout.

Par conséquence on peut conclure que notre nouvelle architecture (Trust AODV) présente un renforcement de sécurité avec un impact minimal sur les performances. Cependant elle est encore empirique et présente encore de faiblesses.

CONCLUSION GÉNÉRALE

Le problème de la sécurité dans le domaine des réseaux est un problème décisif car les données transmises sont potentiellement sensibles et il est souvent aisé de les intercepter ou de les manipuler, notamment dans un réseau ouvert tel que les MANETs où chaque nœud joue le rôle supplémentaire de routeur.

Les réseaux ad hoc présentent des challenges difficiles dans la sécurisation du routage. D'après l'étude que nous avons faite dans le premier chapitre de ce mémoire, les réseaux ad hoc se caractérisent par des qualités qui les distinguent des réseaux filaires. Dans un premier temps, certaines de ces qualités peuvent représenter des avantages, mais ils peuvent constituer un handicap dans des situations particulières. De ce fait et vu leurs spécificités, les MANETs sont plus vulnérables à l'intrusion par rapport aux autres types de réseau ainsi deux aspects sont critiques et importants se produisent : la sécurité des données transmises et en particulier la sécurité du routage ad hoc qui est vulnérable à plusieurs attaques.

Les protocoles de routage ad hoc sont spécifiés sans aucune mesure de sécurité, ils présupposent que tous les nœuds coopèrent et sont « de bonne foi ». Pourtant, les services de sécurité sont identifiés comme essentiels pour assurer un déploiement large de ces réseaux.

Au cours de ce mémoire, nous avons présenté les bases de la sécurité et de passer en revue les différentes technologies actuelles pour les réseaux Ad hoc en mettant l'accent sur les vulnérabilités et les solutions de sécurité correspondantes. Des solutions différentes de sécurité sont proposées ; cependant, elles peuvent s'avérer parfois insuffisantes contre certains comportements malveillants des nœuds et parfois être sujette à certaines menaces. Aucune de ces solutions ne résout complètement le problème de sécurité dans les réseaux Ad hoc et chacune possède ses avantages, et ses inconvénients.

Les MANETs nécessitent des mécanismes pour sécuriser les communications et se protéger contre l'écoute clandestine. Il s'agit donc de concevoir de nouveaux mécanismes afin de garantir la sécurité de ces réseaux. De plus, à cause de plusieurs contraintes telles que l'absence d'une infrastructure et l'absence d'une relation de confiance préalable en même temps provoquent des difficultés pour définir une structure de sécurité stable que l'on le

désire. La difficulté majeure réside dans le fait que cette structure doit être adaptée aux spécificités des MANETs.

Parmi les solutions de sécurité proposées nous avons distingué une approche très intéressante consiste à utiliser des techniques de protection de la vie privée dans les systèmes de gestion de confiance que nous avons apporté dans notre contribution pour protéger les données privatives des différents participants au système.

Pour aborder la problématique de sécurité au niveau des mécanismes de routage, nous avons proposé une architecture distribuée et auto-organisée nourrie par les interactions des nœuds avec son environnement et adaptée aux réseaux sans fil Ad hoc. Nous avons commencé par trouver une solution de surveillance basée sur l'écoute de voisinage commun qui protège le trafic du contrôle contre las attaques. Ce mécanisme de surveillance est renforcé par l'usage d'un modèle de confiance et de réputation distribué et coopératif. Le mécanisme de l'écoute de voisinage permet de diviser le réseau ad hoc en plusieurs zones auto-organisées pour en faciliter la surveillance et la gestion. Cette solution nous a servie pour bâtir nos propositions de gestion de confiance dans des réseaux ad hoc à base du protocole de routage AODV.

Durant l'analyse des simulations, nous avons évalué la résistance de notre architecture de confiance face aux certains types d'attaques. Notre solution donne des résultats satisfaisants en termes de détection et de performance (la dégradation des performances est raisonnable). Mais, cette amélioration nécessite une modification au niveau des messages de contrôle du protocole AODV, et de présenter de nouveaux messages pour le processus de surveillance. Cette opération représente un handicap pour l'avancement des mesures, parce qu'elle demande un temps de plus. Notre architecture proposée n'est pas robuste à toutes les situations d'usage et pose encore plus de questions.

Pour but de ne pas ralentir les communications, notre objectif sera dans le future de trouver d'autres solutions qui minimisent davantage les coûts en termes de communication et de calcul, tout on assure un routage fiable et sécurisé et maintenir un niveau de confiance entre les nœuds.

BIBLIOGRAPHIE

[1] S. Taneja and A. Kush, “A Survey of Routing Protocols in Mobile Ad Hoc Networks”, IJIMT, Vol. 1, No. 3, ISSN2010-0248, August 2010.

[2] E. Conchon, “ Définition et Mise en Oeuvre d’une Solution d’Emulation de Réseaux Sans Fil”, thèse de Doctorat en informatique et télécommunications, l’Institut National Polytechnique, TOULOUSE, 2006.

[3] M. Rajesh Babu, S. Selvan, “An Energy Efficient Secure Authenticated Routing Protocol for Mobile Adhoc Networks”, AJSR, ISSN 1450-223X9(10), pp.12-22, 2010.

[4] A. Banerjee and P. Dutta, “Binary Location-Search Based Scalable Routing Protocol For Ad Hoc Networks”, (IJCNC) Vol.2, No.5, September 2010.

[5] M. Abdelmadjid Allali et Z. Mekkakia Maaza, “Modélisation des Réseaux Ad hoc par Graphes”, 5th International Conference: SETIT 2009 – TUNISIA.

[6] R. Beaubrun et B. Molo, “ Évaluation du Délai dans un Réseau Mobile Ad Hoc Multi-Services”, IEEE 978-1-4244-1643-1/08, 2008.

[7] V. Gayraud, L. Nuaymi, F. Dupont, S. Gombault, and B. Tharon “La Sécurité dans les Réseaux Sans fil Ad Hoc”, SSTIC03 ,2003.

[8] T.LEMLOUMA. “Le Routage dans les Réseaux Mobiles Ad Hoc”, Université Houari Boumediene, Institut d'Informatique, Mini projet, Septembre 2000.

[9] S.WU, “Protocoles de Diffusion dans les Réseaux Ad Hoc Sans fil”, thèse de Doctorat en informatique et Télécommunications, Télécom Paris (ENST), 2004.

[10] Jean-Marc Percher et Bernard Jouga. “Détection d'Intrusions dans les Réseaux Ad Hoc”, SSTIC'03, Rennes, juin 2003.

[11] R. Badonnel, “ Supervision des Réseaux et Services Ad-Hoc ”, thèse de Doctorat en informatique, Université Henri Poincaré – Nancy 1, 2006.

[12] N. Garg, R.P.Mahapatra, “MANET Security Issues”, IJCSNS, VOL.9 No.8, August 2009.

[13] C. YAWUT, “Adaptation à la Mobilité dans les Réseaux Ad Hoc”, thèse de Doctorat en informatique et Télécommunications, Institut National Polytechnique, TOULOUSE, 2009.

[14] Y. M. Ghamri-Doudane, S-M. Senouci et G. Pujolle, “Contrôle des Réseaux Ad Hoc à Base de Politiques”, CFIP, 2002.

[15] K. Beydoun, “Conception d’un Protocole de Routage Hiérarchique pour les Réseaux de Capteurs ”, thèse de Doctorat en informatique, U.F.R des Sciences et Techniques, Université de Franche-Comte, 2009.

[16] T. Clausen, U. Herberg, “Multipoint-to-Point and Broadcast in RPL”, ISRN INRIA/RR--7244--FR+ENG, April 2010. URL: http://www.thomasclausen.org/Thomas_Heide_Clausens_Website/Research_Reports_files/rr-7244.pdf (consulté le 30/05/2012).

[17] I. JEMILI, “Clusterisation et Conservation d’énergie dans les Réseaux Ad Hoc Hybrides à Grande Echelle”, thèse de Doctorat en informatique, Université de Bordeaux I, 2009.

[18] Abderrahmen Mtibaa, “Etude des Performances du Protocole MMDV: Multipath and MPR based AODV”, CFIP-POSTER-02, 2002.

[19] Julien Thomas, “Détection de la Malveillance et Réactions dans les Réseaux Ad Hoc – Bibliographie”, 2007. URL: http://master.julienthomas.eu/rapports/rapportBiblio.pdf (consulté le 30/05/2012).

[20] Y.C. Hu, A. Perrig, D.B. Johnson, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks”, infocom03, 2003.

[21] H. YANG, H. LUO, F. YE, S. LU, L. ZHANG, “Security in Mobile Ad Hoc Networks: Challenges and Solutions”, IEEE Wireless Communications, February 2004.

[22] C. Burgod, “Contribution à la Sécurisation du Routage dans les Réseaux Ad Hoc”, thèse de Doctorat en informatique, Université de Limoges, 2009.

[23] V. UNTZ, “Les Réseaux Sans Fil Spontanés pour l’Internet Ambiant”, thèse de Doctorat en informatique, INP Grenoble, 2007.

[24] Eddy Cizeron, “Routage Multichemins et Codage `a Description Multiple dans les Réseaux Ad Hoc”, Thèse de Doctorat en Automatique et Informatique Appliquée, Université de Nantes, 2009.

[25] F. GUIDEC, “ Déploiement et Support à l’Exécution de Services Communicants dans les Environnements d’Informatique Ambiante”, thèse en vue de l’obtention du diplôme d’habilation à diriger des recherches en informatique, Université de BRETAGNE SUD, 2008.

[26] Charles E. Perkins, ravin Bhagwat, “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers”, SIGCOMM 94 - 8/94 ACM 0-89791 -682-4/94/0008, London, 1994.

[27] U. Ashraf, “Qualité de Service et Routage dans les Réseaux Maillés Sans Fil”, thèse de Doctorat en informatique, Université de TOULOUSE, 2010.

[28] F. SAILHAN, “Localisation de Ressources dans les Réseaux Ad Hoc”, thèse de Doctorat en informatique, Université de PARIS VI, 2010.

[29] M. Sedrati, L. Aouragh, L. Guettala, A. Bilami, “Etude des Performances des Protocoles de Routage dans les Réseaux Mobiles Ad-Hoc”, 4th ICoCIM CIP’2007, 03-04 November 2007.

[30] I.GAWEDZKI, “Routage Multi chemin et QdS dans les Réseaux Ad Hoc Mobiles”, Rapport de stage de Master Recherche Informatique, Université de Paris-Sud, 2004.

[31] F. JADDI, “CSR : une Extension Hiérarchique Adaptative du Protocole de Routage Ad Hoc DSR”, thèse de Doctorat en informatique et Télécommunications, INP de Toulouse, 2006.

[32] S. Maag, C. Grepet, A. Cavalli, “Un Modèle de Validation pour le Protocole de Routage DSR”, CFIP 2005, 18 janvier 2005.

[33] I. Gawedzki, “Algorithmes Distribués pour la Sécurité et la Qualité de Service dans les Réseaux Ad Hoc Mobiles”, thèse de Doctorat en informatique, Université de PARIS-SUD 11, 2008.

[34] Malika BELKADI, “Contrôle de Flux Capable de s’adapter à l’état d’un MANET”, Thèse de Doctorat en Informatique, Université de Tizi Ouzou. URL:http://www.ummto.dz/IMG/pdf/These_Belkadi-2.pdf (consulté le 30/05/2012).

[35] X. Xue, “Mécanismes de Sécurité pour des Protocoles de Routage des Réseaux Ad Hoc”, thèse de Doctorat en informatique, Ecole Nationale des Télécommunications Paris, 2006.

[36] M. Mehdi, A. Anou, S. Zair, M. Bensebti et M. Djebari, “La Sécurité dans les Réseaux Ad Hoc”, SETIT– TUNISIA, March 25-29, 2007.

[37] Abderrezak RACHEDI, “Contributions à la Sécurité dans les Réseaux Mobiles Ad Hoc”, Thèse de Doctorat en Informatique, Université d’Avignon et des Pays de Vaucluse, 2008.

[38] C. Sreedhar, S. Madhusudhana Verma, N. Kasiviswanath, “A Survey on Security Issues in Wireless Ad hoc Network Routing Protocols”, IJCSE Vol. 02, No. 02, 2010.

[39] J. Lebegue, C. Bidan, B. Jouga, “Les Réseaux Ad Hoc et leurs Problématiques de sécurité”, crisis05, 2005.

[40] A. Jangra, N. Goel, Priyanka, K. Bhatia, “Security Aspects in Mobile Ad Hoc Networks (MANETs): A Big Picture”, IJEE, 2010.

[41] X. Li, A. Nayak, I. Ryl, D. Simplot, “On Secure Mobile Ad hoc Routing”, Ad Hoc & Sensor Wireless Networks Vol. 00, pp. 1–26 (aswin62), 2007/9/21.

[42] D. Martins, H. Guyennet, “ Etat de l’art Sécurité dans les réseaux de capteurs sans fil”, SAR-SSI, 2008. URL : http://lifc.univ-fcomte.fr/~publis/hal/mg08:np.pdf (consulté le 30/05/2012).

[43] Emmanouil A. Panaousis, C. Politis, “Securing Ad-hoc Networks in Extreme Emergency Cases”. URL: http://dircweb.king.ac.uk/papers/Panaousis2010_52592293/Secure%20Routing%20for%20Supporting%20Ad-hoc%20Extreme%20Emergency%20Infrastructures.pdf (consulté le 30/05/2012).

[44] N. Bhalaji, S. banerjee, A. Shanmugam, “A Novel Routing Technique against Packet Dropping Attack in Adhoc Networks”, JCS 4 (7): 538-544, 2008.

[45] Yi-an Huang, Wenke Lee, “A Cooperative Intrusion Detection System for Ad Hoc Networks”, URL :http://wenke.gtisc.gatech.edu/papers/sasn.pdf (consulté le 30/05/2012).

[46] A. Vora, M. Nesterenko, S. Tixeuil, S.Delaët, “Universe Detectors for Sybil Defense in Ad Hoc Wireless Networks”, URL : http://deneb.cs.kent.edu/~mikhail/Research/detectors.sss08.pdf (consulté le 30/05/2012).

[47] Zongwei Zhou, “Security Enhancement Over AD-HOC AODV Routing Protocol”, CNIS07, 2007.

[48] L. Abusalah, A. Khokhar, and M. Guizani, “A Survey of Secure Mobile Ad Hoc Routing Protocols”, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 10, NO. 4, FOURTH QUARTER 2008.

[49] P. Nie, “Security in Ad hoc Network”, Helsinki University. URL : http://www.tcs.hut.fi/Studies/T-79.7001/2007SPR/nie_paper_draft.pdf (consulté le 30/05/2012).

[50] Abdesselem BEGHRICHE, “De la Sécurité à la E-Confiance basée sur la Cryptographie à Seuil dans les Réseaux sans fil Ad hoc”, Mémoire de magister en informatique, Université de Batna, 2009.

[51] Seila Nuon, “Analyse de la Disponibilité dans les Réseaux Ad Hoc”, 2006. URL :ftp://ftp.idsa.prd.fr/local/caps/DEPOTS/BIBLIO2006/Rapbiblio-Nuon-Seila.pdf (consulté le 30/05/2012).

[52] Boussad AIT-SALEM, “ Sécurisation des Réseaux Ad hoc : Systèmes de Confiance et de Détection de Répliques”, Thèse de Doctorat en Informatique, Université de Limoges, 2011.

[53] Pietro Michiardi, “Coopération dans les Réseaux Ad Hoc : Application de la Théorie des Jeux et de l’Evolution dans le Cadre d’Observabilité Imparfaite”, SSTIC06, 2006.

[54] Othmane REZINE, “Sécurité des Protocoles de Routage des Réseaux AD HOC ”, mémoire de PFE en informatique, Ecole Superieure des communications de Tunis, 2005.

[55] Noureddine CHAIB, “ La Sécurité des Communications dans les Réseaux VANET”, Mémoire de magister en informatique, Université de Batna.

[56] URL: http://lesdefinitions.fr/confiance (consulté le 30/05/2012).

[57] URL: http://eduscol.education.fr/ecogest/si/SSI/dossierSSI/files/risk-conf.pdf (consulté le 30/05/2012).

[58] Boussad Ait-salem ‘‘Sécurité des Calculs Distribués Multiparties Application : Sécuriser le Calcul Distribué des Confiances.’’, MajecSTIC, 2009.

[59] J. Lebegue, B. Jouga et C. Bidan, “ Etat de l’art sur la Sécurité des Réseaux Ad Hoc”, 2005. URL: http://www.rennes.supelec.fr/ren/perso/jlebegue/docs/Etat_art.pdf (consulté le 30/05/2012).

[60] J.Viji Gripsy et A. Saro Vijendran ‘‘A Survey on Security Analysis of Routing Protocols’’, GJCST Volume 11 Issue 6 Version 1.0 April2011.

[61] Y. Lin, A. H. Mohsenian Rad, V. W.S. Wong,J. Song ‘‘Experimental Comparisons between SAODV and AODV Routing Protocols’’, LRWSc05, 2005.

[62] H. Sh.Jassim, S. Yussof, T. Sieh Kiong, S. P. Koh, R. Ismail ‘‘A Routing Protocol based on Trusted and shortest Path Selection for Mobile Ad hoc Network’’, IEEE 9th Malaysia ICC, 2009.

[63] L. Tamilselvan, V. Sankaranarayanan ‘‘Prevention of Blackhole Attack in MANET’’, IEEE 2nd ICWBUWC (AusWireless 2007)0-7695-2842-2/07, 2007.

[64] M. Anuar Jaafar, Z. Ahmad Zukarnain ‘‘Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment’’, EJSR ISSN 1450-216X Vol.32 No.3, pp.430-443, 2009.

[65] E. Altman et T. Jiménez‘‘NS Simulator for Beginners’’, Université de Los Andes, Mérida Venzuela et ESSI, 2004. URL : http://www-sop.inria.fr/members/Eitan.Altman/COURS-NS/n3.pdf (consulté le 30/05/2012).

[66] L. Cedrik, A. Pascal, ‘‘Distribution d'une Interface de Modélisation pour Ns-2’’, Rapport de stage Master 1 (STIC), Université de la Réunion (UFR) France, 2010.